Universal Service Administrative Co.

Solicitation for Enterprise Data Platform – ~~1st~~ 2nd Revision

SOLICITATION INFORMATION:

Method of Solicitation:	Request for Proposal ("RFP")
Solicitation Number:	IT-26-148
Solicitation Issue Date:	Monday, October 12, 2026
Question Due Date:	Tuesday, October 20, 2026
Q&A Response Due Date:	~~Monday~~Friday, October ~~26~~30, 2026
Proposal Due Date:	Monday, ~~November 23~~December 7, 2026

CONTRACT TO BE ISSUED BY:

Universal Service Administrative Co.
700 12th Street, NW, Suite 900
Washington, DC 20005

CONTACT INFORMATION:

USAC CONTACT INFORMATION	OFFEROR CONTACT INFORMATION
Mustafa Kamal Procurement Specialist P: 202-423-2615 E: Procurement@usac.org Mustafa.Kamal@usac.org	(complete) Name: _____ POC: _____ POC Title: _____ POC Phone: _____ POC Email: _____ Address: _____

Universal Service Administrative Co.

SECTION A:

ABOUT US

1. ABOUT USAC

Through its administration of the Universal Service Fund ("USF") programs on behalf of the Federal Communications Commission ("FCC"), the Universal Service Administrative Company ("USAC") works to promote the availability of quality telecommunications services at just, reasonable, and affordable rates, and to increase access to advanced telecommunications services throughout the nation. Specifically, the USF programs provide funding for the expansion of telecommunications and broadband access to rural communities and health care facilities, schools and libraries, and low-income households. Through program administration, auditing, and outreach, USAC works with contributors, service providers, and program beneficiaries to achieve the program goals articulated by the FCC for the High Cost Program, Lifeline Program, Rural Health Care Program, and Schools and Libraries Program.

USAC strives to provide efficient, responsible stewardship of the programs, each of which is a key national asset in making important telecommunications and Internet services available to consumers, health care providers, schools, and libraries throughout the United States. The program divisions are supported by additional USAC personnel in other divisions, including Finance, Office of General Counsel ("OGC"), Information Systems, Audit and Assurance, Enterprise Process Improvement ("EPI"), and Human Resources ("HR").

Consistent with FCC rules, USAC does not make policy nor interpret unclear provisions of statutes or the FCC's rules. The USF is funded by contributions from telecommunications carriers, including wireline and wireless companies, and contributions from interconnected voice over internet protocol ("VoIP") providers, including cable companies that provide voice service, based on an assessment of their interstate and international end-user revenues. These contributions are typically passed through to consumers through a universal service fee line item on their telephone bills.

High Cost Program

The High Cost Program is designed to ensure that consumers in rural, insular, and high-cost areas have access to modern communications networks capable of providing voice and broadband service, both fixed and mobile, at rates that are reasonably comparable to those in urban areas ("High Cost"). High Cost fulfills this universal service goal by allowing eligible carriers who serve these areas to recover some of their costs from the USF. Like all USF programs, the administration of High Cost has undergone significant modernization in the last several years to increase innovation and ensure beneficiaries have access to updated technology. USAC developed and now leverages the High Cost Universal Broadband Portal ("HUBB"), which allows participating carriers to file deployment data showing where they are building out mass-market, high-speed internet service by precise location. This information includes latitude and longitude coordinates for every location where service is available, and USAC displays this information on a public-facing map to show the impact of high-cost funding on broadband expansion throughout the United States.

Universal Service Administrative Co.

Lifeline Program

The Lifeline Program provides support for discounts on broadband and voice services to eligible low-income households ("Lifeline"). USAC uses its centralized application system, the Lifeline National Eligibility Verifier ("National Verifier"), to verify consumer eligibility through proof of income or the consumer's participation in a qualifying federal benefit program, such as Medicaid, the Supplemental Nutritional Assistance Program ("SNAP"), Federal Public Housing Assistance, or Veterans and Survivors Pension Benefit. USAC focuses on metrics and data analytics for Lifeline improvement and provides outreach efforts to eligible households to increase participation in and the effectiveness of Lifeline. USAC also works to ensure program integrity by supporting the needs of Lifeline stakeholders, reducing program inefficiencies, and combating waste, fraud, and abuse. USAC reviews processes regularly to increase compliance, identify avenues for operational improvements, and refine program controls, such as audit processes.

Rural Health Care Program

The Rural Health Care Program supports health care facilities in bringing medical care to rural areas through increased connectivity ("RHC"). RHC consists of two main component programs: (1) the Telecommunications Program ("Telecom") and (2) the Healthcare Connect Fund Program ("HCF"). The FCC established Telecom in 1997 to subsidize the difference between urban and rural rates for telecommunications services. Under Telecom, eligible rural health care providers can obtain rates on telecommunications services in rural areas that are reasonably comparable to rates charged for similar services in corresponding urban areas. In 2012, the FCC established HCF to promote the use of broadband services and facilitate the formation of health care provider consortia that include both rural and urban health care providers. HCF provides a discount on an array of advanced telecommunications and information services such as Internet access, dark fiber, business data, traditional DSL, and private carriage services. These telecommunications and broadband services support telemedicine by ensuring that health care providers can deliver cutting edge solutions and treatments to Americans residing in rural areas.

Schools and Libraries Program (E-Rate)

The Schools and Libraries Program helps schools and libraries obtain high-speed Internet access and telecommunications services and equipment at affordable rates ("E-Rate"). E-Rate provides a discount for the cost of broadband and telecommunications services to and within schools and libraries in order to support a modern and dynamic learning environment. Applicants and service providers submit FCC Forms (e.g. requests for services or funding) and other compliance-related documentation to the E-Rate Productivity Center ("EPC"), an electronic platform that enables participation in the program. USAC frequently invests in new tools and data analytics capabilities to support the success of the program in alignment with the FCC's goals.

Contributions

Universal service support is money collected from telecommunications companies and then dedicated to fulfilling the goals of universal service. Universal service is paid for by contributions from telecommunications carriers, including wireline and wireless companies, and interconnected VoIP providers, including cable companies that provide voice service, based on an assessment of their interstate

and international end-user revenues. Telecommunications companies are required by law to make contributions to the USF, paying in a percentage of their end-user interstate and international revenues.

All telecommunications companies must register with USAC, whether they contribute to the USF directly or through their underlying carriers. All intrastate, interstate, and international providers of telecommunications (including VoIP providers) within the United States, with limited exceptions, are legally obligated to file the FCC Forms 499.

The term "telecommunications" refers to the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Additional information on USAC programs can be found at: USAC | About | Universal Services.

2. COMPANY PROFILE

USAC is a not-for-profit Delaware corporation operating under the oversight of the FCC. USAC is not a federal agency, a government corporation, a government-controlled corporation or other establishment in the Executive Branch of the United States government. USAC is not a contractor to the federal government. The Contract (as defined in Section C.1.D of this RFP) awarded as a result of this RFP will not be a subcontract under a federal prime contract. USAC does, however, conduct its procurements in accordance with the terms of a Memorandum of Understanding with the FCC, which requires USAC to adhere to the following provisions from the Code of Federal Regulations: 2 C.F.R. §§ 200.318-321; 200.324; 200.326-327 and App. II to C.F.R. Part 200 (collectively "Procurement Regulations").

3. CONFIDENTIALITY

This RFP is subject to the terms of the Confidentiality Agreement (attached hereto as **Attachment 2**) which must be executed by Offeror and submitted along with any proposal for this RFP. Any contract for awarded work under this RFP will also be subject to the terms of such Confidentiality Agreement.

4. OFFEROR AND CONTRACTOR DESIGNATION

Any party that provides a bid and proposal to this RFP is considered an "Offeror". Any Offeror that is awarded work under this RFP and enters into a contract with USAC to deliver the awarded work is considered a "Contractor".

Universal Service Administrative Co.

SECTION B:

STATEMENT OF WORK

1. OVERVIEW

Contractor shall provide a modern, cloud-native, FedRAMP Moderate (or higher) authorized enterprise data platform and the professional services necessary to design, validate, implement, operate, and transition that platform as the Universal Service Administrative Company's ("USAC") enterprise analytical foundation. Contractor shall furnish all management, supervision, labor, licensing, hosting, tooling, processes, and associated support necessary to deliver the requirements of this Section B: Statement of Work.

The Enterprise Data Platform ("EDP") shall replace USAC's existing on-premises Vertica-based Enterprise Data Warehouse ("EDW") and shall provide an integrated set of capabilities supporting enterprise data ingestion, integration, transformation, storage, modeling, governance, metadata management, data quality, semantic modeling, analytics, geospatial processing, artificial intelligence enablement, and operational monitoring. The EDP shall consolidate enterprise data from USAC business systems into a centralized, governed analytical environment that improves data quality, accessibility, transparency, resiliency, and decision-making across the organization.

The Statement of Work consists of three (3) distinct parts that are defined by three (3) separate Contract Line Item Numbers ("CLINs"). In CLIN 001, Contractor shall provide software and licensing as described below for the EDP. Licenses shall be held in USAC's name. In CLIN 0002, Contractor shall provide services to install and configure the platform, and migration services as described in the sections below. In CLIN 0003, Contractor shall provide Hypercare followed by Operations and Maintenance Support.

2. TYPE OF CONTRACT

The contract to be awarded pursuant to this RFP will be a hybrid of Firm-Fixed Price ("FFP") and Time and Materials ("T&M") single award contract ("Contract"). The FFP and T&M price for the work (total project and all line items) is to be set forth in Attachment 1 (Bid Sheet) to this RFP that Offeror completes and returns to USAC as part of Offeror's proposal. The contract pricing will include all direct and indirect costs set forth in this RFP, including equipment, product support, supplies, and general and administrative expenses, overhead, materials, travel, labor, taxes (including use and sales taxes), shipping, and profit. Offerors must provide separate pricing in Attachment 1: Bid Sheet for each CLIN as follows:

CLIN	Description	Pricing Method
0001	Platform licensing, hosting, and storage	~~Annual~~ FFP
0002	System implementation, migration, and cutover	FFP

Universal Service Administrative Co.

CLIN	Description	Pricing Method
0003	Hypercare, operations and maintenance, and transition-out	T&M with annual not-to-exceed ("NTE") ceiling
	Overall NTE to deliver all three (3) CLINs (CLINs 0001 – 0003)	To be presented as an overall NTE

3. CONTRACT TERM

The term of the Contract shall be for a base period of one (1) year with two (2) one-year renewal options ("Contract Term"), unless extended by USAC or terminated sooner in accordance with the Contract. The Contract Term shall commence on the first day of the awarded Contract period of performance (the "Effective Date") as set forth in the awarded Contract. USAC may exercise an option year by written notice to Contractor no less than thirty (30) days prior to expiration of the then-current base year or option year period.

4. PLACE OF PERFORMANCE

4.1. All required Services (as defined in Section C.1.U) under the awarded Contract must be performed within the United States at either USAC's headquarters at 700 12th Street NW, Suite 900, Washington, DC 20005 ("USAC Headquarters"), virtually, or such other location as USAC may approve in its sole discretion. Presently, USAC has a hybrid work approach requiring Contractor Staff (as defined in Section C.1.G) to be in the USAC office at least two (2) days per week. Contractors that are required to report in person must reserve their workspaces in designated areas in advance using USAC's hoteling system.

4.2. Contract kick-off meeting may be held at USAC Headquarters or virtually. USAC will not reimburse Contractor for any travel-related expenses for kick-off, status, and other meetings.

4.3. Contractor shall schedule, coordinate, and hold a Contract "Kick-Off Meeting" no later than ten (10) workdays after any Contract award, at USAC Headquarters or virtually as approved by USAC. The Kick-Off Meeting will provide an introduction between Contractor Staff and USAC personnel who will be involved with the awarded Contract. The meeting will provide the opportunity to discuss technical, management, and security issues, and review Contractor's proposed project timeline and reporting procedures. At a minimum, the attendees shall include Key Personnel (as described in Section C.1.N), Contractor Staff capable of obligating the Contractor, and USAC personnel.

4.4. Services requiring work at USAC Headquarters will include appropriate workspace and appropriate access to USAC's computer network. NOTE: To access USAC IT Systems, Contractor must sign USAC's IT Security Rules of Behavior Form and complete mandatory IT Security and Privacy Awareness Online Training. Contractor Staff will be required to complete Role-Based Privacy Act Training prior to accessing any USAC information system designated as

Universal Service Administrative Co.

a federal system of records (i.e., National Verifier and National Lifeline Accountability Database), including any environment into which data from such a system has been replicated.

4.5. Status update meetings and other meetings may be held virtually, except to the extent that USAC or Contractor requires in-person presence and will be held in accordance with USAC and Contractor's Continuity of Operations Plan ("COOP"). While attending USAC Headquarters for meetings or to conduct audits, Contractor Staff will be considered visitors. All visitors are required to complete USAC's Visitor Form and wear a badge while on premises. Contractor may also be required to attend meetings at the FCC offices located at 45 L Street NE, Washington, DC 20554.

4.6. Upon written request by USAC, Contractor shall provide a COOP including business continuity plans, disaster recovery plans, emergency operations plan and procedures, and associated plans and procedures in the event performance must be conducted virtually or system/software is down.

5. BACKGROUND AND CURRENT STATE

The information in this Section B.5 is provided to establish a common baseline for all Offerors. Detailed inventories, volumetrics, data models, interface control documentation, and security control documentation are available in the Virtual Reading Room described in Section B.13 following execution of Attachment 2: USAC Confidentiality Agreement.

5.1. Current Platform

USAC operates an on-premises Enterprise Data Warehouse built on Vertica. The environment comprises three (3) environments: Development (three (3) nodes), UAT (four (4) nodes, approximately 600–700 GB), and Production (five (5) nodes). The data architecture is organized into three (3) layers: L1 (raw/staging), L2 (operational data store / standardized), and L3 (EDW / analytical reporting). Extract, transform, and load ("ETL") processing is performed using Pentaho Data Integration ("PDI"). Business intelligence is delivered through Tableau Server and Tableau Desktop. Posit Server is available to provide and share advanced analysis. Data cataloging and metadata management are performed in Collibra. Geospatial capability is provided through ESRI Enterprise, ArcGIS Pro, and QGIS. Public data publication is performed through Socrata (Tyler Technologies) at opendata.usac.org.

5.2. Volumetrics

Attribute	Current State
Total structured data under management	Approximately 10–13 TB against 26 TB licensed capacity
Daily ingest volume	Approximately 50–100 GB per day
Tables loaded daily	Approximately 9,750

Attribute	Current State
Tables in L1 and L2	Approximately 4,563, of which approximately 1,282 undergo daily full truncate-and-load
Data type transformation	Approximately 10% of tables undergo data type transformation between L1 and L2
Historical depth in active storage	In excess of twenty-five (25) years
ETL processing window	Approximately 5:00 PM through 10:00 AM the following day
Peak CPU utilization period	3:00 AM – 10:00 AM, sustained above 75%
Largest observed reporting query	26.5 billion rows scanned to produce 88 rows of output
Certified Tableau Data Sources	59 (SL 16, LI 11, Enterprise 4, RHC 9, Finance 12, HC 7)
Lifeline subscriber records	In excess of 20 million enrolled subscribers, hosted on AWS RDS PostgreSQL

5.3. Source Systems and Integration Points

Source systems include transactional applications built on SQL Server, PostgreSQL, and MariaDB, together with manual and file-based feeds (CSV, spreadsheet). Enterprise applications include Oracle E-Business Suite (the USAC financial system, "UNIFi") and Microsoft Dynamics 365 ("CRM"). Program operational systems include, without limitation, the High Cost Universal Broadband Portal ("HUBB"), the Lifeline National Eligibility Verifier ("National Verifier"), the National Lifeline Accountability Database ("NLAD"), the Representative Accountability Database ("RAD"), the Lifeline Claims System ("LCS"), the E-Rate Productivity Center ("EPC"), and Rural Health Care systems including RHC Connect. External feeds are received from the FCC and other federal sources and include, without limitation, the Death Master File, SAM.gov data, census data, and location fabric data supporting the High Cost Program. USAC leverages AWS API Gateway for Application Programming Interface ("API") management and Okta as its enterprise identity provider.

5.4. Documented Limitations of the Current Environment

The following limitations have been identified through internal review and successive independent assessments and constitute the principal drivers of this procurement. Offerors are expected to demonstrate how their proposed solution addresses each:

- The current EDW lacks failover capability. Nightly incremental backups permit restoration from the prior three (3) days, with an estimated restoration time of one (1) to three (3) days.

There is no standby environment. This exposes ERP and Open Data operations to extended outage.

- The architecture tightly couples storage and compute, preventing on-demand scaling during the peak processing window and producing query timeouts and job failures under concurrent ETL and reporting load.
- Reporting relies substantially on a normalized data model inherited from source applications rather than one designed for analytical use. Large join operations spanning twenty (20) to thirty (30) tables cause disk spillover. No table partitioning exists.
- In excess of two (2) decades of data resides in the active storage layer, degrading performance and increasing backup, storage, and governance cost. No documented disposition process exists for electronic records.
- ETL scheduling is time-triggered rather than dependency-driven. A single record-level error causes the entire job to fail. Job failures are reviewed manually during business hours and re-run from the beginning. There is no dedicated production support function.
- Source system schema and data changes are not consistently communicated in advance, causing downstream job failures and delayed data availability.
- GIS data is not integrated with the EDW owing to platform geospatial limitations, requiring separate handling and manual effort for geoprocessing workloads. In addition, the current platform does not allow for connections to USAC's current GIS desktop software.
- Metadata is ingested into Collibra automatically via Collibra's metadata connectors. No complete enterprise business glossary or data dictionary exists.
- Data quality management is reactive. There is no enterprise data quality tooling, rule set, scorecard, or root cause analysis process. Issues are typically discovered when an anomaly is observed.
- Tableau connects to the database through a shared service account, preventing attribution of queries to individual users. A majority of programs report from the L2 layer, which is not optimized for reporting.
- Master data management is not implemented. A prior implementation attempt using Microsoft Master Data Services was not operationalized.
- Platform-specific skills are increasingly scarce, complicating hiring, retention, and support scaling.

5.5. Out of Scope

The following are expressly outside the scope of this Statement of Work:

- Replacement of transactional systems of record.
- Custom application development unrelated to data platform enablement.
- On-premises-only solutions.
- Rebuilding, re-platforming, or re-engineering the UNIFi (Oracle E-Business Suite) interfaces. USAC will assume responsibility for any required changes to those interfaces using internal resources. Contractor shall, however, deliver and maintain the data products that source those interfaces, in accordance with Section B.6.6.



- Development and delivery of end-user training curricula, train-the-trainer programs, or instructor-led training. Knowledge transfer, documentation, runbooks, standard operating procedures, and transition materials are in scope and are addressed in Sections B.7.3.3 and B.7.3.4.
- Implementation of a master data management solution. The platform shall provide master data management capability for future use, as set forth in Section B.6.10.

6. PLATFORM CAPABILITY REQUIREMENTS

Contractor shall provide a commercially available, cloud-native, Software-as-a-Service enterprise data platform meeting the requirements of this Section B.6. The core platform capability shall be delivered through a single FedRAMP Moderate or higher authorized offering under a single authorization boundary. Solutions assembled from multiple separately authorized third-party components to satisfy the core platform capability are not responsive to this requirement; this does not preclude integration with USAC's existing enterprise tooling, nor the use of additional authorized services operating within the same authorization boundary as the proposed offering.

Unless otherwise specified, all capabilities described in this Section shall be provided as native platform functionality or through vendor-supported configuration. Solutions requiring extensive custom software development or unsupported third-party components to satisfy these requirements are discouraged and will be evaluated accordingly.

6.1. Mandatory Requirements

The requirements in this Section B.6.1 are mandatory. Offerors must certify that the proposed platform satisfies each mandatory requirement. Only proposals certifying compliance with all mandatory requirements will be considered for further evaluation, unless no Offeror is able to comply with one or more of them, in which event USAC reserves the right to remove the requirement in question and proceed with the evaluation.

- The core platform capability is delivered through a single FedRAMP Moderate or higher authorized offering, under a single authorization boundary, authorized at the time of award.
- The platform is cloud-native and delivered as a Software-as-a-Service or vendor-managed service; on-premises-only solutions are not responsive.
- All USAC Data, including primary, backup, and disaster recovery copies, is hosted within the United States, and USAC has visibility at all times into where its data is hosted and into the Contractor personnel who interact with it.
- The platform securely ingests data from USAC source environments, including PostgreSQL, SQL Server, and MariaDB, and from file-based feeds, and supports log-based Change Data Capture.
- The platform ingests, stores, indexes, and analyzes geospatial data alongside non-spatial enterprise data within the same governed environment.
- The platform generates and manages an enterprise metadata catalog and maintains end-to-end, column-level lineage.

- The platform integrates with USAC's Okta identity provider for single sign-on and enforces role-based, row-level, and attribute-based access control evaluated at query execution time.
- The platform applies dynamic data masking and tokenization to designated sensitive attributes without requiring duplication of datasets.
- The platform provides transparency into the physical and logical data models holding USAC Data, such that USAC personnel can determine which structures to query.
- The platform supports analysis, modeling, and reporting through native capability, documented native integrations, or documented APIs, using standard connectivity protocols including Java Database Connectivity ("JDBC"), Open Database Connectivity ("ODBC"), and Representational State Transfer ("REST").
- The platform operates on a 24x7x365 basis with high availability and disaster recovery meeting the recovery objectives in Section B.9.3.
- The platform is elastic and scales storage and compute independently to accommodate changing USAC requirements.
- The platform is built on technology with a broad commercial user base and an established professional services market, such that USAC is able to obtain implementation and support resources from more than one source over the Contract Term and beyond it.

6.2. Data Ingestion and Processing

The platform shall provide scalable, cloud-native capability for ingesting, processing, transforming, and managing enterprise data from diverse internal and external sources. At a minimum, the platform shall:

- Support ingestion of structured, semi-structured, and unstructured data.
- Support batch, scheduled, event-driven, log-based Change Data Capture ("CDC"), and near-real-time ingestion patterns.
- Provide native CDC capability against PostgreSQL, SQL Server, and MariaDB sources through vendor-supported configuration or graphical interfaces, without requiring extensive custom development, and without placing intrusive query load on the source database.
- Bind directly to source database logical replication mechanisms and resume from the exact log sequence position following interruption, without causing replication slot growth or storage pressure on the source.
- Support business event-triggered data refreshes initiated through APIs, messaging services, webhooks, event streams, or equivalent cloud-native mechanisms.
- Integrate with USAC enterprise applications, including ERP systems, databases, cloud services, APIs, and file-based data sources.
- Support secure integration with third-party REST APIs and other industry-standard integration protocols.
- Support ingestion pipelines that execute in parallel, and dependency-driven orchestration that releases downstream jobs as soon as their prerequisite data is available rather than upon completion of all upstream processing.
- Provide record-level error handling that isolates failed records to a quarantine or error store and permits the pipeline to continue processing conforming records without a hard stop.

- Support automated retry, restart, and backfill of failed or interrupted jobs without manual intervention, and support replay and reprocessing of prior periods.
- Handle late-arriving data, enforce correct temporal ordering, and perform de-duplication prior to commitment to the analytical layer.
- Support automated schema discovery and schema evolution, absorbing additive source schema changes in flight without pipeline failure or data loss.
- Support data contracts and metadata-driven ingestion.
- Automatically detect structural changes in source systems and notify designated users.
- Provide native workload management that prevents individual users or processes from monopolizing platform resources.
- Support automatic workload balancing and elastic compute scaling to eliminate performance bottlenecks during peak query and ingestion volumes, with isolation between ingestion and analytical workloads.
- Support partitioning, clustering, indexing, storage pruning, and query optimization with minimal administrative intervention, and minimize the need for database administration through automated optimization and performance tuning.
- Provide comprehensive monitoring and alerting for ingestion failures, latency, and pipeline performance.
- Support secure file-based ingestion and egress, including interfacing with a secure file transfer protocol ("sFTP") endpoint, with integrity verification on transfer.
- Provide an audit, balance, and control capability that reconciles record counts, control totals, and checksums between source and target for every load, and that detects and reports incompleteness or drift during and after each refresh rather than only at the point of failure.
- Prevent the introduction of duplicate records through pipeline execution, and permit changes to loaded data only through controlled, logged, and authorized mechanisms.

The platform shall additionally support the ingestion, storage, and governed analysis of unstructured and semi-structured content, and shall provide documented integration with enterprise content management repositories. USAC program operations generate substantial document-based content, including consumer eligibility documentation, form attachments, and review artifacts; Offerors shall describe the platform's capability to bring such content under the same catalog, classification, retention, and access control regime applied to structured data.

USAC does not intend to replicate its existing ETL estate. Pentaho Data Integration shall be fully replaced by native platform ingestion capability. USAC seeks solutions that minimize custom ETL workload; transformation logic in the current environment is limited and exists principally to normalize or de-normalize data to fit the target schema.

6.3. Data Modeling and Semantic Layer

The platform shall provide modern data modeling and semantic modeling capability enabling business users and analysts to consume trusted enterprise data with minimal dependence on IT resources. At a minimum, the platform shall:

- Support logical and physical data modeling.
- Support multiple modeling patterns concurrently across different data domains, including dimensional, data vault, and medallion or lakehouse patterns.
- Provide an enterprise semantic layer that abstracts technical data structures into business-friendly terminology.
- Enable authorized business users to create and maintain semantic models through intuitive graphical interfaces, including drag-and-drop mapping of business terms to physical data structures.
- Support reusable business metrics, calculations, and dimensions.
- Support version control and environment promotion of semantic models and business logic, including integration with Git-based source control.
- Enable rapid deployment of semantic layer changes without extensive redevelopment and provide impact analysis prior to publishing changes.
- Support multiple semantic models over shared data for different business domains while maintaining centralized governance.
- Support role-based presentation of semantic models.
- Support federated data product ownership by program or functional domain within a centralized governance and security framework.
- Support the definition and enforcement of standardized, centrally governed business rules and conformed dimensions and hierarchies, such that the same business concept resolves consistently across program domains.
- Support point-in-time and as-of reporting through temporal history, snapshotting, or equivalent capability, permitting a dataset to be reconstructed and queried as it stood at a prior monthly, quarterly, annual, or funding-year boundary.
- Support slowly changing dimension handling and retention of historical attribute values sufficient to support audit and restatement.

Point-in-time reporting is a substantive requirement rather than a convenience. USAC reports to the FCC, responds to audit inquiry, and supports appeals against the state of program data as of defined dates and funding years. The platform shall support reproduction of a prior reported result without reliance on restoration from backup.

6.4. Data Governance, Metadata, and Lineage

The platform shall provide comprehensive enterprise data governance capability promoting transparency, accountability, and trust in enterprise data assets. Structure 1 is retaining Tableau, and Structure 2 is platform-native reporting. Option A is retaining Collibra as the catalog of record, and Option B is the native catalog. At a minimum, the platform shall:

- Automatically capture technical metadata during ingestion and processing.
- Maintain a centralized, searchable enterprise metadata catalog.
- Support business glossary management.
- Automatically classify enterprise data based on configurable policies, and support metadata tagging and labeling.

- Support configurable stewardship workflows, data ownership assignment, and certification of trusted data assets.
- Maintain complete end-to-end source-to-report lineage, including column-level and transformation lineage sufficient to support audit defensibility.
- Provide visual end-to-end lineage diagrams and maintain historical lineage information.
- Support impact analysis when upstream data structures change.
- Support integration with enterprise governance processes and third-party governance tooling.

6.5. Data Quality and Controls

The platform shall provide enterprise-class data quality management capability. At a minimum, the platform shall:

- Support configurable data quality rules authored by both business users through no-code or low-code interfaces and by engineers through SQL.
- Support automated profiling of source and target data.
- Validate data types during ingestion; detect missing, duplicate, and invalid values; and support referential integrity validation.
- Support tiered enforcement, including hard-stop enforcement for designated critical data elements, warning-level enforcement, and exception-based handling.
- Support configurable threshold-based quality alerting.
- Generate data quality scorecards, trend reporting, and executive-level reporting.
- Support exception management workflows and integration with USAC IT service management tooling.
- Support Unicode character encoding and preserve special characters across ingestion, storage, and reporting.
- Support automated remediation where appropriate.
- Maintain complete audit history of data quality rule execution.

6.6. Analytics, Business Intelligence, and Data Consumption

The platform shall enable secure, governed, and self-service analytical capability. ~~Structure 1 is retaining Tableau, and Structure 2 is platform-native reporting. Option A retains Collibra as the catalog of record, and Option B is the native catalog~~ Contractor to understand that Tableau is USAC's current reporting tool and Colibra is utilized as our catalog of record. Contractor as per Attachment #1 'Pricing Sheet', should provide pricing within CLIN 0002 Detailed Pricing to replace both with platform native tools for reporting and for the data catalog.

At a minimum, the platform shall:

- Support SQL, Python, R, and notebook-based analytical workflows.
- Integrate with Posit Connect or provide natively available capability to host and serve R and Python based models.

- Support standard connectivity protocols, including JDBC, ODBC, REST APIs, and language-native connectors, without proprietary lock-in.
- Enable governed self-service reporting, ad hoc analysis, scheduled reporting, and enterprise dashboards.
- Support secure external data sharing and controlled external publication where authorized, including API-based open data services with rate limiting, egress monitoring, and logging.
- Support high concurrency while maintaining performance, with workload isolation between analytical, ingestion, and data science workloads.
- Support Section 508 and WCAG 2.1 Level AA conformance for any externally facing output.
- Support scheduled report generation and distribution, including delivery by email with the output attached or rendered in the message body, and support bursting of a single report to multiple recipients with row-level filtering applied per recipient.
- Store report and analytical artifacts within the governed environment and permit them to be shared among authorized USAC users securely, with access governed by the same role-based and row-level controls applied to the underlying data.
- Present an interface usable by non-technical business users without engineering assistance for discovery, filtering, and consumption of governed data products.

Offerors may propose retention of Tableau, or consolidation of reporting onto the proposed platform's native capability.

- Offerors shall describe the human-computer interaction characteristics of the proposed platform for each of the principal USAC user populations non-technical business users, program analysts, data engineers, and security administrators and shall identify which tasks in each population's workflow require engineering assistance under the proposed model. USAC will evaluate usability as a substantive factor; a platform whose governed self-service capability is only reachable by technically expert users does not satisfy the intent of this Section.

USAC currently publishes public data through Socrata at opendata.usac.org, for which a license is in place. The platform shall feed Socrata as the baseline publication path. Offerors may propose platform-native external publication as a separately priced and separately evaluated alternate, stating the total cost to USAC and any change to the public consumption experience.

6.7. Artificial Intelligence and Advanced Analytics

The platform shall provide capabilities for enabling responsible adoption of artificial intelligence and machine learning. At a minimum, the platform shall:

- Store, version, and manage machine learning models and model metadata.
- Provide or integrate with vector database capability.
- Support Retrieval-Augmented Generation architectures and semantic search.
- Support integration with Large Language Models.
- Support AI-assisted data discovery, classification, metadata enrichment, and data quality rule suggestion.

- Support natural language query against governed semantic models.
- Support agent-based workflows.
- Support prompt governance, auditing, and guardrails preventing data leakage in generative AI use cases.
- Support AI interoperability through standards-based interfaces. Support for the Model Context Protocol, or an equivalent interoperability standard, is highly desirable.
- Support explainability controls and human review of AI-generated output.

Artificial intelligence capability is a required attribute of the platform. Its use and deployment are separately gated. Contractor shall not use, implement, build, or deploy AI tools, services, or code of any type in performance of this Contract without prior written approval from USAC. Any proposed AI use must be submitted in writing and receive written approval before use. This requirement is a gate on use and production deployment, not a prohibition on assessment, and it does not preclude the assessment and design work under CLIN 0002.

6.8. Geospatial Capability

The platform shall provide enterprise geospatial data management and analytical capability to support USAC's GIS operations. ESRI ArcGIS Enterprise shall remain the authoritative system of record for spatial data; the platform shall receive copies for analytics, reporting, and governed external publication. At a minimum, the platform shall:

- Ingest, store, index, and manage spatial data alongside non-spatial enterprise data within a single governed environment.
- Support common geometry types, including points, lines, polygons, and multipart geometries.
- Support spatial data types, spatial indexing, spatial partitioning, and distributed spatial processing.
- Support spatial joins and spatial analysis at enterprise scale, including point-in-polygon operations intersecting broadband deployment coordinates against federal eligibility boundary polygons such as Tribal lands, census blocks, and FCC location fabric data.
- Support ingestion, validation, and conversion of multiple geometry formats, including but not limited to shapefiles, GeoJSON, KML/KMZ, WKT/WKB, GeoPackage, and Cloud Optimized GeoTIFF.
- Support raster data types and OGC standards, including WMS, WFS, and WCS.
- Support coordinate reference system transformations.
- Support metadata consistent with applicable FGDC and ISO standards.
- Enforce role-based and row-level security controls on spatial data.
- Optimize spatial queries over large enterprise datasets.
- Direct ArcGIS Pro connection to the cloud database

6.9. Data Lifecycle, Retention, and Archival

Contractor shall implement a data lifecycle management capability meeting the following requirements:

- Ten (10) years of data shall be retained in the active analytical schema and shall be queryable without restoration.
- Data older than ten (10) years shall be archived to lower-cost storage with a documented, accessible retrieval path. Archived data shall be restorable to a queryable state within five (5) business days for any dataset up to one (1) terabyte, through a documented request and approval workflow.
- Archived data shall reside within the platform's managed storage. Offerors may propose an alternative archival architecture as a priced alternate, stating the cost, retrieval performance, and governance implications.
- Archival, retention, and disposition shall conform to USAC's records retention policy and to applicable National Archives and Records Administration retention schedules. Contractor shall not destroy any USAC Data without prior written approval from USAC.
- Lineage, catalog entries, and classification metadata shall be preserved for archived data.

6.10. Master Data Management

Implementation of master data management is not required under this Contract. The platform shall, however, provide master data management capability available for future use, including entity resolution, survivorship rules, golden record management, and stewardship workflow. Offerors shall describe this capability and shall state whether it is native to the proposed offering or requires additional licensing.

6.11. Environments, Operations, and Observability

At a minimum, the platform and Contractor shall provide:

- Four (4) isolated environments: Development, Test/QA, Pre-Production, and Production. Pre-Production shall be capable of holding production-representative data volumes sufficient to validate end-to-end processing and reporting performance prior to production deployment.
- Infrastructure as Code for environment configuration and provisioning, and CI/CD pipelines for automated build, test, and deployment of platform changes.
- Comprehensive monitoring, logging, and alerting across ingestion, processing, storage, and consumption, integrated with USAC monitoring and IT service management tooling.
- Cost visibility and FinOps capability, including workload-level cost allocation tagging, consumption dashboards, budget alerting, and resource governance controls capable of constraining runaway compute consumption.
- Documented approach to platform maintenance, version upgrades, and change management, including the maintenance window model and the extent to which upgrades are performed without service interruption.
- The ability for an administrator to create and manage separate project workspaces, sandboxes, analytical labs, data marts, and datasets for multiple teams, with independent access control and cost attribution, and without permitting one team's activity to degrade another's.

- The ability to configure and support multiple data marts and aggregation layers linked to the governed enterprise layer, and to manage varying processing loads and data traffic across them.
- An administrative console providing USAC-designated personnel a high degree of visibility into and control over configuration, operation, workload activity, active data loads, and security posture of the platform, without dependence on Contractor intermediation for routine inspection.
- Capacity monitoring and forecasting sufficient to project future storage, compute, and concurrency requirements as data volume and user population grow.

Contractor shall document, and shall keep current, the network and connectivity architecture on which the platform depends, including the connectivity model between USAC networks and the platform, bandwidth requirements necessary for USAC staff to interact with the platform at performance comparable to the current on-premises experience, and all ports and protocols required. Contractor shall identify every dependency the platform places on USAC-controlled network infrastructure.

Contractor shall disclose whether the platform operates from data centers owned by the Contractor or platform provider, or leased from another provider, and shall identify any sub-processor or third-party infrastructure provider in the delivery chain. Contractor shall notify USAC of any change to those arrangements that could reasonably affect service continuity, data residency, or the authorization boundary. Contractor shall not delegate responsibility for the security of USAC Data to a third-party cloud service provider; Contractor remains accountable to USAC for the security posture of the delivered service irrespective of where it is hosted.

6.12. Cloud Computing Capabilities

At a minimum, the platform shall provide:

- Reserved or guaranteed GPU capacity
- Scaling of GPU/CPU/vRAM capabilities to meet any new recommended requirements with ArcGIS Pro upgrades
- Autoscaling CPU/GPU clusters for batch training, scaling to zero when idle
- Python, R (RStudio/Posit), and Jupyter environments with custom container images

7. SCOPE OF WORK

7.1. CLIN 0001: Platform Licensing, Hosting, & Storage

Under CLIN 0001, Contractor shall provide the platform subscription, hosting, and storage necessary to operate the Enterprise Data Platform in accordance with Section B.6, for the base period and each exercised option year.

7.1.1. Contractor shall provide all platform licensing, subscription entitlements, hosting infrastructure, disaster recovery/failover, compute, and storage required to operate the four

Universal Service Administrative Co.

(4) environments identified in Section B.6.11 at the capacity levels established by the sizing basis provided in the Virtual Reading Room.

7.1.2. Contractor shall deliver the platform within a FedRAMP Moderate or higher authorized boundary. All hosting shall be within the United States. Contractor shall provide the platform within AWS Commercial Cloud (US), ~~or~~ Microsoft Azure, or a USAC-managed tenant under USAC's FISMA ATO. Offerors shall state their current authorization status and the specific authorization boundary within which the proposed offering operates.

7.1.3. will contract directly with the platform provider for the platform subscription, licenses, and associated entitlements, and will hold them in USAC's name. Contractor shall not purchase, hold, or resell platform licenses or subscriptions under this Contract.

(a) Contractor shall identify in its proposal the platform licenses, subscriptions, and entitlements required to meet the requirements of Section B.6 for each environment identified in Section B.6.11, for the base period and each option year. For each item, Contractor shall state the quantity, the license or consumption metric, and the estimated annual cost.

(b) Contractor shall update the license requirements and cost estimate at the conclusion of the POC, and whenever a change in scope, sizing, or consumption would change the licenses USAC needs.

(c) USAC will hold the owner and primary administrator accounts for the platform instance. Contractor shall administer the platform only through accounts and roles that USAC assigns and may revoke at any time.

(d) The platform instance, USAC Data, configurations, infrastructure as code artifacts, and documentation produced under this Contract are USAC's property. Contractor shall not configure the environment in a manner that impairs USAC's ability to administer it, assume operation of it, or assign it to a successor contractor.

~~Where Contractor is not the platform original equipment manufacturer, Contractor shall hold or shall cause to be held in USAC's name or assignable to USAC, the platform subscription and associated entitlements, such that ownership of the platform instance, USAC Data, configurations, and licenses, together with the right to administer them, transfers to USAC or its designee upon expiration, termination, or transition of this Contract. Contractor shall not configure the environment in a manner that impairs USAC's ability to assume or reassign it.~~

~~**7.1.3.** USAC reserves the right to purchase the platform licenses directly from the platform vendor and to own and configure the supporting Contractor specified infrastructure on its owned Cloud instance.~~

Universal Service Administrative Co.

7.1.4. Contractor shall provide consumption and cost reporting sufficient for USAC to monitor spending against the CLIN 0001 ~~annual FFP, and~~FFP and shall notify USAC in writing when projected consumption is forecast to exceed eighty percent (80%) of any contracted capacity threshold.

7.1.5. Contractor shall state the cost model applicable to retrieving, exporting, or transferring USAC Data out of the platform, including any data egress, extract, or transfer charges, and shall recommend practices for minimizing those charges. Contractor shall confirm that no egress, extract, or transfer charge will be applied to the return of USAC Data under Section B.7.3.4 or Section C.17.

7.1.6. Contractor shall state all cost drivers, consumption metrics, and the factors that materially increase or decrease cost, and shall identify which capabilities described in Section B.6 are native to the proposed offering, and which require separate licensing.

7.2. CLIN 0002: System Implementation, Migration, and Cutover

Under CLIN 0002, Contractor shall design, build, migrate, test, and place into production the Enterprise Data Platform in accordance with the target-state architecture, scope definition, and implementation plan developed during the Proof of Concept ("POC") phase and finalized in this CLIN. CLIN 0002 is FFP ~~with an annual not-to-exceed ceiling definitized~~ in accordance with Section B.2.

7.2.1. Design and Build

- Establish and configure the four (4) environments identified in Section B.6.11, including network, identity, security, monitoring integration, and to provide high availability and disaster recovery capability meeting the recovery objectives stated in Section B.9.3
- Implement infrastructure as code, CI/CD pipelines, source control integration, and environment promotion workflows.
- Design and physicalize the target-state data models, including the standardized common data model and the analytical reporting layer.
- Design and implement the enterprise semantic layer.
- Build the ingestion pipelines for all in-scope sources, using native platform capability, and retire the corresponding Pentaho Data Integration jobs.
- Implement dependency-driven orchestration, record-level error handling, quarantine management, automated retry and restart, and backfill and replay capability.
- Implement the data quality framework, including rule authoring, profiling, tiered enforcement, scorecards, alerting, and exception workflow.
- Implement the governance, catalog, lineage, and classification capability.
- Implement geospatial ingestion, indexing, and processing.
- Implement data lifecycle management, including the ten (10) year active retention standard, archival, and the documented retrieval workflow.

- Implement security controls in accordance with Section B.8.2, including single sign-on, role-based, row-level, and attribute-based access control, masking, tokenization, encryption, and audit logging.
- Implement monitoring, logging, alerting, and FinOps capability in accordance with Section B.6.11.

7.2.2. Migration

- Migrate historical data in accordance with Section B.6.9, loading ten (10) years into the active analytical schema and placing older data into archive with a documented retrieval path.
- Migrate reports and semantic models in accordance with the scope defined during the POC period,
- Migrate and re-establish the datasets published to opendata.usac.org, and the disbursement and payment data feed sourcing UNIFi.
- Migrate existing Collibra content.
- Migrate analytical code assets, including R and Python workloads.

7.2.3. Testing, Parallel Operation, and Cutover

- Contractor shall prepare and execute a test plan covering unit, integration, system, regression, performance, stress, disaster recovery, and user acceptance testing, and shall identify for each the respective roles of Contractor and USAC personnel and the tooling used. Performance and stress testing shall be executed against production-representative data volumes in the pre-production environment, and stress testing shall establish the point at which platform performance degrades below the standards in Section B.9. Contractor shall test contingency and continuity procedures and shall remediate, at no additional cost to USAC, any defect identified in testing before USAC approval to proceed to production.

- Contractor shall operate the new platform in parallel with the legacy EDW for a period of not less than ninety (90) calendar days prior to each production cutover, or such longer period as USAC directs. During parallel operation, Contractor shall perform reconciliation between legacy and target outputs and shall report reconciliation results to USAC on a weekly basis.

- Cutover shall be approved by USAC in writing and shall be conditioned upon: (a) reconciliation demonstrating agreement between legacy and target outputs for the ~~mandatory floor~~minimum viable product (MVP) items in Section B.6.6 within the tolerance established in the approved test plan; (b) successful user acceptance testing; (c) successful performance testing against the standards in Section B.9; (d) successful disaster recovery and failover testing against the recovery objectives in Section B.9.3; and (e) delivery and acceptance of operational runbooks and standard operating procedures.

- Contractor shall propose a phased cutover sequenced by data domain. Contractor shall accommodate FCC regulatory reporting cycles and audit windows in the cutover schedule and shall not schedule a cutover event within any reporting window identified by USAC.

7.2.4. Change Management

Contractor shall provide change management support scoped to adoption and communications only. This shall comprise stakeholder engagement, development and execution of a communications plan, definition and tracking of adoption metrics, and go-live readiness assessment. Development and delivery of training curricula, train-the-trainer programs, and instructor-led end-user training are outside the scope of this Contract.

7.3. CLIN 0003: Hypercare, Operations & Maintenance, And Transition-Out

Under CLIN 0003, Contractor shall provide hypercare following each production cutover, ongoing operations and maintenance of the Enterprise Data Platform, and transition-out support. CLIN 0003 is T&M with an annual NTE ceiling definitized in accordance with Section B.2.

7.3.1. Hypercare

Contractor shall provide a hypercare period of not less than sixty (60) calendar days following each production cutover, during which Contractor shall provide elevated support coverage, daily issue triage and reporting, expedited defect resolution, and performance monitoring against the standards in Section B.9. Exit from hypercare requires USAC written acceptance.

7.3.2. Operations and Maintenance

- Provide production support for the platform and all in-scope pipelines, including incident response, break-fix remediation, and root cause analysis in accordance with the service levels in Section B.9.
- Monitor pipeline execution, job status, data freshness, and platform health; proactively identify and remediate failures; and maintain a shared operational dashboard providing USAC stakeholders visibility into job status and failure trends.
- Perform proactive performance tuning, capacity management, partition and index optimization, and query optimization.
- Manage platform patching, version upgrades, and vendor-driven change, coordinated with USAC in accordance with USAC change control procedures.
- Operate the data quality framework, including rule execution monitoring, exception triage, scorecard production, and coordination of remediation with source system owners.

- Maintain governance, catalog, lineage, and classification content as the platform evolves.
- Operate the archival and retrieval workflow in accordance with Section B.6.9.
- Support enhancement and onboarding of additional sources, domains, and data products as directed by USAC.
- Maintain cost visibility and provide FinOps reporting and optimization recommendations.
- Operate a defined release management process covering platform and vendor-driven change, stating how each change is classified, communicated, scheduled, tested, and rolled back, and maintain a forward release and maintenance calendar visible to USAC.
- Maintain and update the capacity plan not less than annually, forecasting storage, compute, concurrency, and cost, and notify USAC in advance of any forecast breach of a contracted capacity threshold.
- Provide platform support to USAC users and administrators, including a defined intake, logging, triage, and escalation process, staffed during core support hours with on-call coverage for P1 incidents outside those hours in accordance with Section B.9.1.
- Provide configurable notification and alerting to USAC personnel through multiple channels, including email and messaging integration with USAC enterprise tooling, for operational, data quality, capacity, and security events.
- Support internal and external audits, including provision of evidence, lineage documentation, and access records.

7.3.3. Documentation and Knowledge Transfer

Contractor shall create and maintain, throughout the Contract Term, current versions of: system and solution architecture documentation; data models and data dictionaries; source-to-target mapping documentation; interface control documentation; operational runbooks; standard operating procedures; incident and escalation procedures; disaster recovery procedures; release documentation; and knowledge base content. Contractor shall conduct knowledge transfer sessions with USAC personnel on a recurring basis sufficient to enable USAC to understand and, if required, assume operation of the platform.

7.3.4. Transition-Out

Contractor shall deliver a Transition-Out Plan no later than ninety (90) days before Contract expiration and a Transition-Out Support Package no later than sixty (60) days before Contract expiration, each meeting the requirements of Section B.10. Contractor shall provide current versions of all documentation, licensing and renewal information, asset and inventory records, operational procedures, in-flight activity status, and shall support shadowing and knowledge transfer sessions necessary to transfer operation to USAC personnel or a successor contractor. Contractor shall not configure or operate the platform in any manner that impairs USAC's ability to assume or reassign it.

Universal Service Administrative Co.

At the conclusion of the Contract, Contractor shall transfer to USAC all USAC Data and all documents produced under the Contract, in a format specified by USAC. Following USAC's written confirmation that the transfer is complete, and subject to Section C.17.B, Contractor shall destroy all remaining copies of USAC Data in its possession or under its control, including copies held by any subcontractor or infrastructure provider, and shall certify the destruction to USAC in writing. Destruction of electronic media shall be performed in accordance with NIST SP 800-88 Rev. 1. Transfer and destruction shall be performed at no additional cost to USAC, and no egress, extract, or transfer charge shall apply.

8. SECURITY, PRIVACY, & COMPLIANCE REQUIREMENTS

8.1. Authorization and Compliance Posture

- The core platform shall hold FedRAMP Moderate or higher authorization at the time of award, under a single authorization boundary. Authorizations described as "in process" do not satisfy this requirement.

- Contractor shall comply with the Federal Information Security Modernization Act ("FISMA") per 44 U.S.C. § 3541 et seq., and with NIST SP 800-53 Rev. 5 security and privacy controls appropriate to the FISMA Moderate impact level.

- Contractor shall support maintenance of System Security Plans, participate in all FISMA assessment activities, support Assessment and Authorization and continuous monitoring activities, provide monthly vulnerability reports, and maintain a Plan of Action and Milestones. Critical and High vulnerabilities shall be reported to the USAC Chief Information Security Officer and remediated within NIST-recommended timeframes.

- Contractor shall facilitate access for third-party penetration testing conducted under USAC's penetration testing contract or successor.

- All hosting shall be within the United States, within AWS Commercial Cloud (US) or Microsoft Azure Commercial or a USAC managed tenant under USAC's FISMA ATO provided that ATO is obtained before production deployment. This applies to primary, backup, and disaster recovery copies of USAC Data.~~All hosting shall be within the United States, within AWS GovCloud (US) or Microsoft Azure Government. This applies to primary, backup, and disaster recovery copies of USAC Data.~~

- Contractor shall hold and maintain, and shall provide evidence of, current independent third-party attestations appropriate to the service, including at a minimum a SOC 2 Type II report. Contractor shall identify any additional certifications maintained, including ISO/IEC 27001 or equivalent.

- Contractor shall permit USAC, or a third party engaged by USAC, to conduct security reviews of the delivered service not less than annually, and shall provide the service control documentation, security policies, and data handling and personnel onboarding and offboarding procedures necessary to support those reviews.

- Where the platform is multi-tenant, USAC Data shall be logically segregated from the data of all other customers, and Contractor shall describe the mechanism enforcing that segregation and the controls preventing cross-tenant access.

8.2. Identity and Access

- The platform shall integrate with USAC's Okta identity provider for single sign-on, supporting SAML 2.0 and OIDC, with multi-factor authentication and conditional access enforcement.
- The platform shall enforce role-based, row-level, and attribute-based access controls, evaluated at query execution time against identity attributes supplied by the identity provider.
- Individual user accounts shall be used for all platform and database access. Shared or generic service accounts shall not be used for interactive or reporting access, and all query activity shall be attributable to an individual identity.
- Access shall follow a least privilege model, with privileged access time-limited and subject to periodic review and recertification.
- The platform shall support USAC's Zero Trust Architecture objectives, including continuous verification, identity-based rather than network-location-based authorization, logical segmentation, and immutable audit logging.
- The platform shall honor USAC's enterprise authentication policy as enforced by the identity provider, including password construction and reuse rules, failed-attempt lockout, and session timeout, and shall not maintain a parallel credential store for users authenticated through the identity provider. Where any local or service credential is unavoidable, it shall be stored using a salted, industry-accepted one-way hash and shall be managed through the approved secrets management solution.
- The platform shall support configurable session inactivity timeout, display of last successful sign-in date and time to the user, and the ability for an administrator to immediately disable or revoke an account or session.
- Authentication and authorization failures shall return minimal information to the requester, and platform error and exception handling shall not disclose internal system detail, stack traces, connection strings, or credentials.

8.3. Data Protection

- USAC Data shall be encrypted at rest and in transit at all times, in accordance with FIPS 140-3 validated cryptography.
- The platform shall support customer-managed encryption keys (BYOK/CMEK) and shall permit USAC to revoke platform access to data through key control.
- The platform shall provide dynamic data masking and tokenization applied at query execution time based on identity attributes, without requiring duplication of datasets.

- The platform shall support data masking and tokenization for data in transit during ingestion as well as at rest.
- Personally identifiable information shall be protected in accordance with the Privacy Act of 1974, OMB M-17-12, and NIST SP 800-53 Rev. 5. The Lifeline Program processes consumer eligibility data including names, addresses, and income verification records; these attributes shall be subject to masking, encryption, and restricted access controls.
- Contractor shall comply with USAC's data classification policy and handle all data in accordance with the classification level assigned by USAC (Public / For Internal Use Only / Confidential / Restricted). The platform shall support enforcement of controls differentiated by classification level.

8.4. Audit Logging and Monitoring

- The platform shall generate immutable, tamper-evident audit logs covering authentication, authorization, query execution, data access, administrative action, configuration change, and policy change.
- Audit logs shall be retained in accordance with USAC's records retention policy and shall integrate with USAC's security information and event management platform.
- The platform shall support user access reporting sufficient to support periodic USAC access review and recertification.
- Each audit log record shall include, at a minimum: source IP address; user account identifier; date and time stamp; event source; device or client information; the outcome of the event as success or failure; and any supplemental information relevant to the event.
- The platform shall prevent modification or deletion of audit records by any unauthorized role, ~~including administrative roles,~~ and shall support export of audit records to a readable, analyzable format.
- The platform shall permit an authorized role to configure the inclusion or exclusion of auditable event types in accordance with USAC policy and operating limits, and shall support querying of audit records by criteria including user, event type, and date range.
- The platform shall support configurable alerting on audit conditions indicating potential misuse, including repeated failed authentication, anomalous query volume, bulk extraction, and access attempts against data classified as Confidential or Restricted.
- Audit and logging functions shall not materially degrade production platform performance.
- Contractor shall maintain procedures for guarding against, monitoring for, and detecting malicious software affecting the platform and any data ingested into it, and shall report detections affecting USAC Data to USAC.

8.5. Resiliency

The platform shall provide high availability and disaster recovery capability meeting the recovery objectives stated in Section B.9.3. Contractor shall document the resiliency architecture, shall test failover and recovery in accordance with Section B.9.3 prior to cutover, and shall test recovery on a recurring basis thereafter as directed by USAC.

Universal Service Administrative Co.

8.6. Secure Development

- Contractor shall integrate automated security scanning, including static and dynamic application security testing, software composition analysis, and dependency scanning, into all delivery pipelines.
- Contractor shall implement a USAC-approved secrets management solution. Hardcoded credentials, API keys, tokens, or secrets in source code are strictly prohibited, and all repositories shall be scanned for exposed secrets.
- Contractor shall implement branch protection controls, including mandatory review before merging to production branches and automated enforcement of quality gates.
- All Contractor Staff performing development under this Contract shall complete annual secure coding training, at minimum covering OWASP Top 10 awareness, secrets management, and applicable NIST secure development guidance. Evidence of completion shall be provided to USAC upon request.

8.7. Personnel Security

- All Contractor Staff performing work under this Contract shall be United States persons.
- All Contractor Staff shall be subject to background investigation prior to being granted access to USAC IT Systems. Contractor Staff with access to USAC systems shall maintain their status throughout the Contract Term, and any adverse finding or change in status shall be reported to USAC's Security Officer within one (1) business day.
- All Contractor Staff accessing USAC IT Systems shall sign USAC's IT Security Rules of Behavior Form and complete mandatory IT Security and Privacy Awareness Online Training.
- Contractor Staff accessing any USAC information system designated as a federal system of records, or any environment containing data replicated from such a system, shall complete Role-Based Privacy Act Training prior to access.

9. PERFORMANCE STANDARDS, SERVICE LEVELS, AND KEY PERFORMANCE INDICATORS

Contractor shall perform all services under this Section B in accordance with the performance standards, Service Level ~~Agreements ("~~Agreements ("SLAs"), and Key Performance Indicators ("KPIs") set forth in this Section. Contractor shall establish and maintain a performance management process supporting routine monitoring of service outcomes, trending of operational data, identification of deficiencies, and implementation of corrective action where performance falls below required standards. Contractor shall track and report SLA compliance in the Monthly Status Report. Persistent SLA failures may constitute grounds for corrective contract action, including termination for cause.

9.1. Incident Service Levels

The following SLA targets apply to production and pre-production environments for all in-scope systems and pipelines.

Universal Service Administrative Co.

Priority	Definition	Initial Response	Resolution Target	Escalation to USAC PM
P1 – Critical	Production platform down; complete loss of service; failure of a ~~mandatory floor~~minimum viable product data product	Within one (1) hour of detection	Within four (4) business hours	Immediately, within one (1) hour of detection
P2 – High	Major functional impairment; significant degradation affecting multiple users or programs	Within two (2) hours of detection	Within eight (8) business hours	Within two (2) hours of detection
P3 – Medium	Limited functional impact; workaround available	Within one (1) business day	Within five (5) business days	Within one (1) business day
P4 – Low	Cosmetic issue or minor enhancement request	Within three (3) business days	Per release schedule	Within three (3) business days

Contractor shall operate a production support capability staffed during core support hours ~~of~~ from Monday through Friday, 9:00 a.m. to 6:00 p.m. ET, excluding federal holidays, and shall maintain on-call capability outside core hours for P1 incidents. P1 incidents shall be worked on a 24x7 basis until service is restored or an acceptable workaround is in place. USAC makes the final determination of incident priority and defect severity. Contractor shall provide, and keep current, a written escalation procedure naming the individuals and senior managers to whom an unresolved incident escalates at each tier, with their titles and direct contact details, and shall follow that procedure where an incident is not responded to or resolved within the stated targets. For each P1 incident, Contractor shall follow USAC's production incident process, provide timely status communications, restore service in accordance with the targets above, perform root cause analysis, and submit an After-Action Report.

9.2. Platform and Data Service Levels

Measure	Target
Platform availability (production, excluding approved maintenance windows)	99.9% monthly
Completion of the daily batch processing cycle	Complete by 6:00 a.m. ET, or such other time established at CLIN 0002 design acceptance

Measure	Target
Data freshness — near-real-time and CDC tiers	Within three hundred (300) seconds of source commit
Data freshness — batch tier	In accordance with the tiered freshness schedule agreed at CLIN 0002 design acceptance
Archived data restoration to queryable state	Within five (5) business days for any dataset up to one (1) terabyte
Pipeline job success rate	99% of scheduled executions per month completing without manual intervention
Deliverable timeliness	100% of deliverables submitted by the agreed due date

9.3. Recovery Objectives

The platform shall meet a Recovery Time Objective ("RTO") of four (4) hours and a Recovery Point Objective ("RPO") of one (1) hour for the production environment. Contractor shall document how the proposed architecture achieves these objectives, shall validate them through failover testing prior to cutover, and shall re-validate them at a frequency directed by USAC thereafter.

9.4. Key Performance Indicators

Contractor shall track and report the following KPIs, which USAC may refine as operational needs mature:

- Platform availability and unplanned outage count and duration.
- Mean time to detect, acknowledge, respond, contain, and resolve, by priority.
- Percentage of incidents triaged and resolved within SLA.
- Pipeline job success rate, failure count, mean time to recovery, and count of failures requiring manual intervention.
- Batch cycle completion time against target, and trend.
- Data freshness achieved against target, by tier.
- Data quality scorecard results by domain, rule execution volume, exception volume, and exception aging.
- Query performance percentiles for governed semantic model access, and count of queries exceeding defined thresholds.
- Catalog and lineage coverage as a percentage of in-scope data assets.
- Report migration progress against the rationalization plan, by category.
- Consumption and cost against contracted capacity, by workload and domain.

- Percentage of deliverables submitted on time, and staffing continuity rate for Key Personnel.

9.5. Acceptance Criteria and Corrective Action

USAC will only accept Services or Deliverables that meet the acceptance criteria described in this Statement of Work, in the approved POC Test Plan, and in the approved CLIN 0002 test plan. USAC shall have ten (10) business days from receipt to accept or reject any deliverable. Rejected deliverables must be corrected and resubmitted within five (5) business days at no additional cost to USAC. Where performance falls below required thresholds, Contractor shall identify the cause of the deficiency, propose corrective action, implement approved remediation, and report progress until the issue is resolved.

9.6. Quality Control

Contractor shall establish, implement, and maintain a Quality Control Plan subject to USAC approval, addressing defined quality objectives and performance standards; internal inspection, testing, and verification procedures; corrective and preventive action processes; document control and version management; subcontractor oversight; escalation procedures for risks, defects, and non-conformances; and reporting cadence. USAC reserves the right to review and require changes to the Quality Control Plan.

9.7. Maintenance, Change, and Outage Notification

Contractor shall perform no change to the production platform environment without first informing USAC. Contractor shall provide not less than two (2) weeks' advance written notice of any planned maintenance, upgrade, or configuration change that could cause service interruption or alter platform behavior, and shall schedule such activity outside the daily processing window and outside any FCC reporting window identified by USAC. Emergency changes shall be communicated as soon as the need is identified, and in any event within twenty-four (24) hours of the change. Contractor shall state, for each planned change, the expected duration of any interruption, the affected components, the rollback plan, and the user impact.

Any service disruption arising from a change that was not communicated to USAC in accordance with this Section shall be treated as a Priority 1 incident under Section B.~~12~~9.1, irrespective of its technical severity, and shall be subject to the associated response, resolution, escalation, and After-Action Report obligations.

10. DELIVERABLES

Contractor shall prepare, maintain, and submit all deliverables required under Section B in accordance with the timelines, formats, and review procedures established by USAC. Deliverables shall be complete, accurate, current, and of sufficient quality to support operational oversight, performance management, risk management, continuity of operations, and transition. All deliverables shall be submitted in a USAC-approved electronic format unless otherwise directed. Formal acceptance is contingent upon USAC's written acceptance. Where a deliverable is described as a living document,

Universal Service Administrative Co.

Contractor shall maintain it throughout the period of performance and document material changes in the applicable recurring status report.

References to months below are months from Notice to Proceed ("NTP") for the applicable CLIN unless otherwise stated.

10.1. Deliverables Summary

No.	CLIN	Deliverable	Frequency / Due	Purpose / Contents
1	All	Kick-Off Meeting	One-time, NLT ten (10) workdays after award	Introduction of teams, review of Contractor approach, technical, management and security discussion, review of timeline and reporting procedures.
2	All	Project Management Plan	One-time, NLT fifteen (15) business days after award; updated as needed	Management approach, reporting structure, communications methods, quality approach, staffing oversight, risk and issue management, PM@USAC alignment.
3	All	Quality Control Plan	One-time; updated as changes warrant	Methods and controls ensuring quality, consistency, timeliness and accuracy; corrective and preventive action; escalation procedures.
4	All	Integrated Master Schedule	One-time, NLT twenty (20) business days after award; updated monthly	All active and planned workstreams, milestones, dependencies and deliverables, subject to USAC PM approval.
5	All	Escalation Procedure and Contact Register	One-time, NLT fifteen (15) business days after award; updated upon any change	Named individuals and senior managers at each escalation tier, with titles and direct contact details, per Section B.12.
6	0002	Environment Build and Configuration Documentation	Per environment, upon completion	Configuration, infrastructure as code artifacts, network and identity integration, monitoring integration, and environment promotion procedures.

Universal Service Administrative Co.

No.	CLIN	Deliverable	Frequency / Due	Purpose / Contents
7	0002	Physical Data Models and Data Dictionary	Upon completion; maintained thereafter	Physicalized target-state models with entities, attributes, relationships, constraints and definitions, including conformed dimensions, hierarchies and governed business rules.
8	0002	Source-to-Target Mapping	Per domain, upon completion; maintained thereafter	How data from each source is transformed and loaded into the target platform, at column level.
9	0002	Audit, Balance and Control Design	One-time prior to first cutover; maintained thereafter	Reconciliation controls, control totals and completeness checks applied to every load, and the reporting through which incompleteness or drift is surfaced.
10	0002	Test Plan and Test Cases	One-time prior to test execution; updated per phase	Unit, integration, system, regression, performance, stress, disaster recovery and user acceptance testing, with acceptance criteria, reconciliation tolerances, and Contractor and USAC roles.
11	0002	Parallel Run Reconciliation Report	Weekly during parallel operation	Reconciliation of legacy and target outputs, variance analysis, and remediation status, with specific treatment of the ~~mandatory floor~~minimum viable product items in Section B.6.6.
12	0002	Performance and Stress Benchmark Report	Prior to each cutover	Measured performance against Section B.9 standards in the Pre-Production environment at production-representative volume, and the point of performance degradation established through stress testing.
13	0002	Disaster Recovery and Failover Test Report	Prior to first cutover; annually thereafter	Failover and recovery test results measured against the RTO and RPO in Section B.9.3, with remediation of any shortfall.

Universal Service Administrative Co.

No.	CLIN	Deliverable	Frequency / Due	Purpose / Contents
14	0002	Cutover Plan and Readiness Assessment	Prior to each cutover	Cutover sequence, rollback plan, communications, go/no-go criteria and readiness evidence against Section B.9.3.
15	0002	Change Management and Communications Plan	One-time; updated as needed	Stakeholder engagement approach, communications plan, adoption metrics and go-live readiness. Excludes training curricula and instructor-led training.
16	0002	Architecture, Network and Interface Control Documentation	Prior to first cutover; maintained thereafter	Current system, solution and network architecture documentation and interface control documents for all in-scope integrations.
17	0003	Hypercare Exit Report	Upon conclusion of each hypercare period	Issue volume and disposition, performance against Section B.9, outstanding defects and readiness for steady-state operation.
18	All	Bi-Weekly Status Report	Bi-weekly	Work performed in the prior period; major activities, issues, risks, staffing updates and operational developments; planned work for the next period with impacts highlighted.
19	All	Monthly Status Report	Monthly	Comprehensive summary of accomplishments, open issues, risks, staffing changes and planned activities; SLA and KPI compliance; supports the monthly invoice.
20	0003	KPI and SLA Dashboard	Ongoing	Management-ready dashboard presenting service levels, performance trends, pipeline health, data quality and reporting timeliness per Section B.9.4.
21	0003	Data Quality Scorecard	Monthly	Data quality results by domain, rule execution volume, exception volume and aging, trend analysis and remediation status.

Universal Service Administrative Co.

No.	CLIN	Deliverable	Frequency / Due	Purpose / Contents
22	0003	Consumption and FinOps Report	Monthly	Consumption and cost by workload and domain against contracted capacity, with optimization recommendations and forecast.
23	0003	Capacity Plan	Annually; updated upon material change	Updated forecast of storage, compute, concurrency and cost, with advance notice of any projected breach of a contracted capacity threshold.
24	0003	Maintenance and Release Calendar	Ongoing; updated not less than monthly	Forward schedule of planned platform maintenance, upgrades and configuration changes, with expected interruption, affected components, rollback plan and user impact, per Section B.9.7.
25	0003	After-Action Report	Per P1 incident	Timeline, impact, root cause, resolution and preventive actions for each Priority 1 production incident.
26	All	Meeting Minutes and Briefing Materials	As directed / recurring meetings	Agendas, minutes, briefing materials and action item summaries for management, operational and coordination meetings.
27	All	Quarterly Performance Review Briefing	Quarterly	Service performance, key trends, risks, accomplishments, improvement areas and recommendations.
28	All	Transition-Out Plan	One-time, NLT ninety (90) days before Contract expiration	Approach for transferring services, documentation, assets, knowledge and responsibilities to USAC or a successor contractor.
29	All	Transition-Out Support Package	One-time, NLT sixty (60) days before Contract expiration	Current documentation, licensing and renewal information, asset and inventory records, procedures, in-flight activity status, and knowledge transfer support.

No.	CLIN	Deliverable	Frequency / Due	Purpose / Contents
30	All	Data Return and Destruction Certificate	Upon completion of transition-out	Confirmation that all USAC Data and Contract documents have been returned in the format specified by USAC, and written certification that remaining copies have been destroyed in accordance with NIST SP 800-88 Rev. 1, at no cost to USAC.

11. KEY PERSONNEL AND LABOR CATEGORIES

Contractor shall provide qualified personnel with the knowledge, skills, experience and certifications necessary to perform all requirements under Section B and shall maintain sufficient depth of staffing to ensure continuity of operations. Additionally, USAC strongly prefers that all Key Personnel are employees of the Contractor and have been so for a minimum of three (3) years. Please provide detailed information about the following Key Personnel, who will be written into the Contract by name:

11.1. Key Personnel

Role	Responsibilities and Minimum Qualifications
Program Manager	Primary point of contact for all programmatic matters. Responsible for overall contract performance, coordination, staffing oversight, risk and issue management, quality oversight, communications and management reporting. A ~~M~~minimum twelve (12) years managing enterprise data or systems integration programs of comparable scale is preferred. PMP or equivalent required. Must be available within two (2) business hours of USAC contact. See labor category description tab on bid sheet for detailed JD
Solution Architect	Accountable for the end-to-end target-state architecture, its conformance to USAC enterprise architecture standards, and its realization through implementation. Leads the POC design and the Technical Design Document. Minimum twelve (12) years in data architecture with at least five (5) years designing cloud-native analytical platforms at enterprise scale. Demonstrated experience with the proposed platform required. See labor category description tab on bid sheet for detailed JD
Data Modeling Lead	Accountable for the conceptual, logical and physical data models, the standardized common data model, the analytical layer and the enterprise semantic layer. Minimum twelve (12) years in enterprise

Role	Responsibilities and Minimum Qualifications
	data modeling with demonstrated experience across multiple modeling patterns, including dimensional and data vault or lakehouse approaches, and experience remediating inherited normalized transactional models for analytical use. See labor category description tab on bid sheet for detailed JD
Migration Lead	Accountable for data, pipeline, report and code migration; parallel operation; reconciliation; and phased cutover. Minimum twelve (12) years leading data platform migrations, with demonstrated experience migrating from a legacy on-premises analytical database to a cloud-native platform and executing reconciliation-gated cutover. See labor category description tab on bid sheet for detailed JD
Security Lead	Accountable for the security and privacy posture of the delivered platform, including identity integration, access control design, masking and tokenization, encryption and key management, audit logging, and support to FISMA and continuous monitoring activities. Minimum twelve (12) years in information security with demonstrated experience in FedRAMP and FISMA environments. CISSP or equivalent required. See labor category description tab on bid sheet for detailed JD
Change Management Lead	Accountable for stakeholder engagement, the communications plan, adoption metrics and go-live readiness assessment. Scope is limited to adoption and communications; this role does not encompass training curriculum development or instructor-led training delivery. Minimum twelve (12) years in organizational change management supporting enterprise technology deployments. See labor category description tab on bid sheet for detailed JD
Senior Business Intelligence Architect	Accountable for the semantic layer and consumption architecture, the comparative evaluation of Structure 1 and Structure 2 described in Section B.6.6, report rationalization design, and natural language query enablement. Works under the Solution Architect, who retains accountability for the end-to-end platform architecture. Minimum twelve (12) years in business intelligence and semantic modeling, including demonstrated experience leading a large-scale business intelligence migration and consolidating reporting estates of comparable size. See labor category description tab on bid sheet for detailed JD
Senior DevSecOps Engineer	Accountable for continuous integration and continuous delivery pipelines, infrastructure as code, automated security scanning within the delivery pipeline, secrets management, and environment promotion across the four (4) environments identified in Section B.6.11. Works

Role	Responsibilities and Minimum Qualifications
	alongside the Security Lead, who retains accountability for security posture, controls design, and FISMA and continuous monitoring activities. Minimum twelve (12) years in DevSecOps or platform engineering, with a relevant current certification such as AWS Certified DevOps Engineer, Microsoft Certified: DevOps Engineer Expert, Certified Kubernetes Administrator, or equivalent. See labor category description tab on bid sheet for detailed JD
Senior Data Warehouse QA/Test Engineer	Accountable for the test plan and test cases required under Sections B.7.2.3 and B.20.2, reconciliation testing, parallel-run validation, and data quality verification across migration. Minimum twelve (12) years in data warehouse and data platform testing, including demonstrated experience with reconciliation-gated cutover and with validating migrated reporting output against a legacy source of truth. See labor category description tab on bid sheet for detailed JD

11.2. Additional Labor Categories

Contractor shall propose and maintain labor categories sufficient to perform all services required under this Section B. At a minimum, Contractor shall provide personnel in labor categories substantially equivalent to the following: Platform Engineer; Data Engineer; Integration Engineer; Geospatial Engineer; Semantic Layer / Business Intelligence Developer; Data Governance Analyst; Data Quality Analyst; DevOps Engineer; Test Lead; Test Analyst; Business Analyst; Technical Writer. Offerors may propose equivalent labor categories with different internal titles provided the proposed personnel meet or exceed the minimum qualification standards described above; any such substitution must be clearly identified and justified in the technical proposal. See labor category description tab on bid sheet for detailed job descriptions.~~JD~~

11.3. Staffing Continuity and Substitution

Contractor shall maintain staffing continuity sufficient to ensure uninterrupted performance and shall provide backup coverage for Key Personnel and critical operational roles. Contractor shall notify USAC in advance of any proposed substitution of Key Personnel and shall provide the qualifications of any proposed replacement. Replacement personnel shall possess qualifications equal to or greater than those of the individual being replaced, unless otherwise approved. Replacement personnel are considered Key Personnel.

USAC reserves the right to require the removal from performance under this Contract of any Contractor Staff, upon written notice with an explanation, and Contractor shall assign an acceptable substitute. Contractor shall not reassign or substitute personnel assigned to the Contract without USAC's prior written approval. Substitute personnel shall not automatically receive the rate of the individual being replaced; the rate for substitute personnel shall be agreed between USAC and Contractor and shall not exceed the rate stated in the Contract for that labor category.

Universal Service Administrative Co.

11.4. USAC Staffing and Division of Work

Contractor shall advise USAC on the number, role, skill set, and level of effort of USAC personnel required to support each phase of the work and to use and oversee the platform in steady state. Contractor shall state, for every task area in this Section B, the proposed division of work between Contractor Staff and USAC personnel, and shall identify any task for which Contractor assumes USAC will supply personnel, a third-party professional services provider, or a capability USAC does not currently hold. Assumptions about USAC-supplied effort that are not stated in the proposal will not be recognized as a basis for schedule relief or additional compensation.

12. APPLICABLE LAWS, DIRECTIVES, AND STANDARDS

Contractor shall perform all services under this Section B in accordance with applicable statutes, regulations, executive directives, federal cybersecurity and privacy guidance, and generally accepted industry practice. USAC may update, supplement, or refine these references during performance to reflect changes in law, policy, or operational requirements.

- Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3541 et seq.
- Privacy Act of 1974, and OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.
- OMB Circular A-130, Managing Information as a Strategic Resource.
- Executive Order 14028, Improving the Nation's Cybersecurity.
- NIST Cybersecurity Framework (CSF) 2.0.
- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations.
- NIST SP 800-53 Rev. 5 and NIST SP 800-53B, Security and Privacy Controls and Control Baselines.
- NIST SP 800-61, Incident Response Recommendations and Considerations for Cybersecurity Risk Management.
- NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization.
- NIST SP 800-92, Guide to Computer Security Log Management.
- NIST SP 800-137, Information Security Continuous Monitoring.
- NIST SP 800-218, Secure Software Development Framework.
- NIST AI Risk Management Framework, and successor and related NIST publications on artificial intelligence.
- OMB M-21-31, M-22-01, M-22-09, M-21-30, M-22-18 and M-23-16, as applicable.
- FIPS 140-3, Security Requirements for Cryptographic Modules.
- FedRAMP requirements and guidance.
- Section 508 of the Rehabilitation Act and WCAG 2.1 Level AA.
- National Archives and Records Administration retention schedules and USAC's records retention policy.
- USAC's Information Security and Privacy Policy, data classification policy, Zero Trust Architecture roadmap, AI governance framework, and change control procedures, as furnished to Contractor.

Universal Service Administrative Co.

13. VIRTUAL READING ROOM AND ATTACHMENTS

USAC will make additional materials available to Offerors in a Virtual Reading Room. To obtain access, Offerors must submit a signed copy of Attachment 2: USAC Confidentiality Agreement to Procurement@usac.org and the USAC contact identified on the cover page. Reading Room materials are Confidential Information subject to Section C.16 and shall govern in the event of any inconsistency with the summary information in Section B.5.

The virtual reading room material will cover the following list:

- Source system inventory, including platform, integration pattern and volumetrics for each in-scope source.
- Sizing basis, including active terabytes, archive terabytes and projected annual growth.
- Table and object inventory, load profile and processing window detail.
- Concurrency figures and user counts by persona.
- Current L1, L2 and L3 data models and available data dictionary content.
- Tableau workbook inventory and usage statistics.
- Interface control documentation for in-scope integrations, including the disbursement and payment data feed sourcing UNIFi.
- USAC Information Security and Privacy Control Policy.
- USAC data classification policy.
- USAC change control procedures and governance model.
- Current-state assessment materials relating to the existing EDW.

14. MEETINGS

During performance of the awarded Contract, Contractor Staff shall communicate on a regular basis with USAC staff and, as requested by USAC's Program Manager or Contracts Administrator, attend status meetings with USAC staff to discuss project status and progress, impediments, and audit findings. Status meetings will be held by either teleconference or in person, and status reports may be used as the basis of the discussion.

Contractor shall schedule, coordinate, and hold a Contract Kick-Off Meeting no later than ten (10) workdays after any Contract award, at USAC Headquarters or virtually as approved by USAC. The Kick-Off Meeting will provide an introduction between Contractor Staff and USAC personnel who will be involved with the awarded Contract, and the opportunity to discuss technical, management, and security issues and review Contractor's proposed project timeline and reporting procedures. At a minimum, attendees shall include Key Personnel, Contractor Staff capable of obligating the Contractor, and USAC personnel.

Meetings that involve or contain disclosure of (a) program participants' PII, (b) confidential information, or (c) contribution data cannot be recorded. If Contractor needs to record a meeting, Contractor must use the teleconferencing software's native recording functionality and obtain USAC's approval prior to any recording. If approved, Contractor must indicate the meeting will be recorded in

the meeting invite and verbally mention it in the meeting and must provide the recording to the appropriate USAC point of contact within one week, in compliance with USAC's Audio and Video Meeting Recording Policy.

15. TRAVEL

Travel expenses are not reimbursable under this Contract.

16. USAC PROGRAM MANAGER AND CONTRACT MANAGER

The Program Manager ("PM") for the Contract is TBD at contract award, the USAC point of contact for overseeing the performance of the Services. USAC's Contracts Administrator ("CA") for the Contract is TBD at contract award, the USAC point of contact for contractual matters (e.g., contract modifications and other contractual matters).

17. USAC TECHNOLOGY AND EMAIL USE

For Contracts requiring access to USAC networks and systems, all Contractor Staff must use their USAC-issued technology to share and store all USAC documents for work purposes. Contractor Staff shall not use external technologies that are not approved by USAC to create, send or view USAC content, documents and/or material.

If USAC issues Contractor Staff an email address (@usac.org), Contractor Staff must use this email address to send and receive all USAC communications and material. USAC documents should not be forwarded or shared to non-USAC email addresses. If confidential USAC information is sent to unauthorized individuals, Contractor must immediately inform their USAC point of contact and immediately complete and submit a Privacy Intake Form (provided upon request). USAC documents shall not be stored in an unauthorized location, personal email, personal cloud, or any portable storage device.

USAC-issued property, including laptops, must not be left unattended and may not be used by anyone aside from the personnel assigned to the USAC-issued property. As part of the offboarding process, Contractor must return all USAC property, whether tangible or intangible including all USAC Confidential Information and Materials in their possession. Contractor must provide written confirmation to USAC that it and its subcontractors have fully complied with this requirement within ten (10) calendar days. In the event of any damage, loss, or theft of tangible or intangible property, Contractor will be held responsible.

18. FOLLOWING PM@USAC POLICY

When applicable, Contractors serving in any capacity as part of a project team must employ PM@USAC as the required project management framework, including the processes, procedures, tools, templates, and artifacts contained within PM@USAC. Any deviations or changes must be approved by PM@USAC.com. PM@USAC, which is a slightly tailored version of the Project Management Institute's PMBOK methodology, is the required project management framework to ensure all projects

Universal Service Administrative Co.

are conducted in a disciplined, well-managed, and consistent manner that promotes the delivery of quality products and services to both internal and external stakeholders.

19. DOCUMENT LABELING AND MANAGEMENT

Contractors are responsible for the protection and proper disclosure of all information, data and documents in their possession or control. Every effort must be made to protect information, documents and all other property entrusted to the Contractor. Every document must have the appropriate marking, such as Confidential/For Internal USAC Use Only.

Contractor must retain all USAC data and documents generated in accordance with USAC's record retention policy and provide those data and documents to USAC upon request or per stated submission instructions in USAC's policies. All retained USAC data and documents must be reasonably accessible and migratable from the system throughout the duration of the contract or required retention period. Upon contract expiration, USAC may request that Contractor migrate any stored USAC data and documents to USAC in a format acceptable to USAC. Contractor shall not destroy documents without written approval from USAC.

20. PROOF OF CONCEPT

To ensure an offeror's proposed solution meets USAC's requirements, USAC requires Proof of Concept (POC) from selected offerors during proposal evaluation, prior to contract award. Offeror should develop and submit a POC Test Plan with its proposal. The purpose of the POC is to establish, on the basis of empirical evidence obtained against USAC's actual data footprint, regulatory overlays, and technical constraints, the information USAC requires to make the following decisions:

- Selection of the target platform and platform vendor.
- Selection of the hosting and tenancy model.
- Definition of the scope and approach for data source/report migration.
- Definition of the scope and approach for data integration and ingestion.
- Definition of the scope and approach for geospatial enablement.
- Definitization of the CLIN 0002 and CLIN ~~0002~~ 0003 NTE ceilings and implementation plan.

20.1. Secure Enclave and Data Handling

- USAC will provide and own the secure enclave within which each Contractor shall perform the POC. The enclave shall reside within a dedicated public sector tenancy, shall be network-isolated from any Contractor commercial cloud environment, and shall be integrated with USAC's Okta identity provider with phishing-resistant multi-factor authentication and conditional access enforcement. Contractor shall not transfer, copy, or replicate USAC Data outside the enclave for any purpose.

- Connectivity between USAC source systems and the enclave shall be established over private network paths, including AWS PrivateLink, VPC endpoints, cross-account VPC peering, or

Universal Service Administrative Co.

equivalent. Data shall not traverse the public internet. Customer-managed encryption keys shall be configured such that USAC retains the ability to revoke platform access to the dataset.

- The POCs shall be executed against a de-identified or synthetic dataset that preserves the referential integrity, cardinality, distribution, and volume characteristics of the production Lifeline and High-Cost datasets, including a subscriber dataset of not fewer than twenty million (20,000,000) records. USAC will supply this dataset. This dataset shall be used for all throughput, concurrency, spatial, schema evolution, late-arriving data, and consumption testing.

- Testing against live, unmasked production data. The purpose of this test is limited to validating dynamic data masking, tokenization, and fine-grained access control behavior and their performance impact under load against production data characteristics.

- Execution of the validation round described in the fourth bullet point above is conditioned upon the following, each of which is a condition precedent: (a) written approval from the USAC Privacy Officer and the USAC Office of General Counsel; (b) completion by all Contractor Staff who will access the enclave of Role-Based Privacy Act Training and USAC IT Security and Privacy Awareness Training; (c) execution by all such Contractor Staff of USAC's IT Security Rules of Behavior Form; (d) completion of a Privacy Impact Assessment where USAC determines one is required; and (e) verification that all such Contractor Staff are United States persons and have satisfied the background investigation requirements of Section B.8.7. Contractor shall not be entitled to schedule relief or additional compensation arising from the time required to satisfy these conditions.

20.2. POC Test Cases:

The POC requires, at a minimum, the following test cases:

- **Ingestion and Change Data Capture**

  Contractor shall establish log-based CDC from a USAC-provided AWS RDS PostgreSQL read replica bound to a logical replication slot, streaming insert, update, and delete mutations continuously. Contractor may elect to stage transaction logs through an intermediate message broker or to connect platform pipelines directly to the replication slot; Contractor shall document the approach, the backpressure handling behavior, and the log sequence number resume behavior following interruption, and shall demonstrate that the approach does not cause replication slot growth or storage pressure on the source replica. USAC will establish the numeric pass thresholds for each test case~~The pass threshold for ingestion latency from source change to target availability is three hundred (300) seconds, without transactional service impact on the source~~.

- **Schema Evolution Resilience**

While the CDC stream is actively pulling mutations, USAC will execute a schema alteration on the source appending a new column, followed immediately by streamed transactions populating that column. The platform shall discover the new attribute, evolve the downstream schema without human intervention, and continue streaming without dropping records or halting the pipeline.

- **Late-Arriving Data, Data Quality, and Quarantine**

  USAC will inject late-arriving records with backdated transactional timestamps, mixed with records containing deliberately malformed values including invalid numeric fields and broken geospatial geometries. The platform shall correctly order the late-arriving records in the analytical layer, apply inline data quality validation, and route malformed records to an isolated quarantine store for audit, without a hard stop to the pipeline.

- **Dynamic Masking, Access Control, and Performance Penalty**

  Contractor shall apply Okta-integrated dynamic data masking and tokenization policies to designated personally identifiable information attributes, and shall demonstrate role-based, row-level, and attribute-based access control enforcement evaluated at query execution time. Contractor shall demonstrate that a restricted role receives tokenized or redacted values while a privileged role receives unmasked values, verified through tamper-evident audit logging. Contractor shall execute concurrent analytical queries against masked and unmasked views and shall report the measured query latency overhead attributable to runtime masking. This test case shall be executed in the parallel round against the de-identified dataset and repeated in the final validation round against live production data

- **Concurrency and Peak Load**

  Contractor shall demonstrate platform behavior under a simulated peak load representative of USAC's 3:00 AM to 10:00 AM window, with concurrent ingestion and analytical query execution. Contractor shall demonstrate elastic scaling, workload isolation preventing analytical load from starving ingestion or financial reporting workloads, and resource governance controls capable of constraining runaway compute consumption.

- **Geospatial Processing**

  Contractor shall ingest, index, and query ESRI shapefiles, GeoJSON, and geometry-bearing columnar formats alongside tabular program and financial data. Contractor shall execute point-in-polygon spatial joins intersecting broadband deployment coordinates against federal eligibility boundary polygons at production-representative scale, and shall report execution time, spatial indexing approach, and optimization technique. Contractor shall demonstrate the mechanism by which optimized spatial views are exposed securely to external map services and to the public data portal.

- **Alternative Data Model Comparison**

Universal Service Administrative Co.

Contractor shall construct and benchmark alternative analytical data models over shared data — including dimensional, data vault, and medallion or Lakehouse patterns — sufficient to inform USAC's target-state modeling decision and shall report comparative query performance and maintenance implications relative to the normalized model inherited from source applications.

- **Governance, Catalog, and Lineage**

  Contractor shall demonstrate automated harvesting of technical, business, and lineage metadata from the platform and connected sources, including column-level and transformation lineage. Contractor shall demonstrate the capability to connect their platform to Collibra.

- **Consumption, Semantic Layer, and Natural Language Query**

  Contractor shall build a governed semantic model over the POC datasets and shall demonstrate: (a) governed self-service consumption by a business user without engineering assistance; (b) business intelligence tool integration using Tableau and platform native capability if applicable; (c) natural language query executed against the governed semantic model, including the governance, auditing, and accuracy controls applied to that capability; and (d) reproduction of a representative sample of existing operational reports identified by USAC, sufficient to establish the effort profile for data source/report migration.

20.3. Discovery and Scoping

Concurrent with the POC, Contractor shall perform the discovery and scoping work necessary to bound CLIN 0002. Preliminary discovery happens during the POC at no cost to USAC. Offerors may include time in CLIN 0002 for detailed discovery and MVP
Contractor shall:

- Produce a source system and pipeline inventory identifying each in-scope source, its platform, its integration pattern (batch, CDC, event-driven, file-based), its volumetrics, and its refresh requirement.
- Define the report migration scope and approach, including identification of semantic model consolidation opportunities and the treatment of the ~~mandatory floor~~minimum viable product set out in Section B.6.6 at the conclusion of the Proof of Concept.
- Define the data integration and ingestion scope and approach, including the disposition of existing Pentaho Data Integration jobs.
- Define the geospatial enablement scope and approach, including the pipeline architecture between ArcGIS Enterprise, the platform, and downstream consumers.
- Identify data lifecycle, retention, and archival requirements against the ten (10) year active retention standard in Section B.6.9.

- Perform a capacity assessment establishing projected storage, compute, concurrency, and cost requirements over the Contract Term and a five (5) year horizon and define the method by which capacity will be reassessed as the platform grows.
- Document the network and connectivity architecture, bandwidth requirements, and all ports and protocols on which the platform depends and identify every dependency on USAC-controlled infrastructure.
- Define the division of work between Contractor and USAC across every phase of CLIN 0002 and CLIN 0003, and state the number, role, skill set, and estimated level of effort of USAC personnel required to support each phase and to operate and use the platform in steady state.

Universal Service Administrative Co.

SECTION C:

USAC Standard Terms and Conditions

1. DEFINITIONS

A. "Added Service" means a service that Contractor may perform for USAC that is not specified in the Scope of Work part of the Contract.

B. "Code" means the United States Bankruptcy Code.

C. "Confidential Information" is defined in Section 16 of these USAC Standard Terms and Conditions.

D. "Contract" means these USAC Terms and Conditions (including the attached USAC Standard Terms and Conditions Privacy and Security Addendum), and any documents attached to these USAC Terms and Conditions that constitutes the entire agreement between the parties with respect to the subject matter hereof.

E. "Contract Term" means the Initial Term of these USAC Standard Terms and Conditions and any executed Optional Renewal Terms.

F. "Contractor" means the Offeror (as defined elsewhere in the Contract) whose proposal was selected for award of the Contract.

G. "Contractor Staff" means Contractor's employees, subcontractors, consultants, and agents used to provide Services and/or create Deliverables under this Contract, including, but not limited to, Key Personnel. "Contractor Staff" also includes the entity that employs Contractor's employees, subcontractors, consultants, and agents in all cases except where the context clearly references only individuals.

H. "Courts" means the district and, if applicable, federal courts located in the District of Columbia.

I. "Deliverables" means the goods, items, products, and materials that are to be prepared by Contractor and delivered to USAC as described in the Contract.

J. "Derivative Works" means any and all modifications or enhancements to, or any new work based on, in whole or in part, any USAC Data, Confidential Information, Software, or Deliverable regardless of whether such modifications, enhancements or new work is defined as a "derivative work" in the Copyright Act of 1976.

Universal Service Administrative Co.

K. "Discloser" means a party to this Contract that discloses Confidential Information to the Recipient.

L. "FCC" means the Federal Communications Commission, including, but not limited to, the Office of the Managing Director, the Office of Economics and Analytics, the Wireless Telecommunications Bureau, the Enforcement Bureau, the Wireline Competition Bureau, and the Public Safety and Homeland Security Bureau.

M. "Initial Term" means the original duration of these USAC Standard Terms and Conditions as described in Section 2 of these USAC Standard Terms and Conditions.

N. "Key Personnel" means the full-time employees of Contractor that are in the positions identified elsewhere in the Contract as those that are required to perform the Services.

O. "Optional Renewal Term" means an additional one year period that can extend the duration of these USAC Standard Terms and Conditions, and that can be exercised at USAC's sole discretion as described in Section 2 of these USAC Standard Terms and Conditions.

P. "Privacy and Security Addendum" means the part of this document that includes most of the language regarding Contractor's obligations around protecting USAC Data.

Q. "Procurement Regulations" mean the following provisions of the Code of Federal Regulations: 2 C.F.R. §§ 200.318-321, 200-324, 200.326-327 and App. II to C.F.R. Part 200.

R. "Recipient" means a party to this Contract that receives Confidential Information from a Discloser.

S. "SAM" means the System for Award Management or suspension or debarment status of proposed subcontractors that can be found at https://www.sam.gov.

~~T. T. "SAN" means the Supplier Actionable Notification, which is a method of paying USAC invoices.~~

~~U.~~T. "Services" means the services, tasks, functions, and responsibilities described in the Contract.

~~V.~~U. "Software" means any application programming interface, content management system or any other computer programs, protocols, and commands that allow or cause a computer to perform a specific operation or series of operations, together with all Derivative Works thereof.

~~W.~~V. "Solicitation" means the request for Services described in the Contract.

~~X.~~W. "Sub-Recipient" means a partner, joint venturer, director, employee, agent, or subcontractor of a Recipient to whom a Recipient must disclose Confidential Information.

Universal Service Administrative Co.

~~Y. "UCSP" means the USAC Coupa Supplier Portal, which is a method of paying USAC invoices.~~

~~Z.~~X. "USAC" means Universal Service Administrative Company.

~~AA.~~Y. "USAC Data" means any data, materials, or communications in any form or format, whether tangible or intangible, spoken or written (regardless of media) provided by USAC to Contractor for use in the performance of the Contract, data that is collected, developed or recorded by Contractor in the performance of the Contract, including without limitation, business and company personnel information, program procedures and program specific information, and Derivative Works thereof. All USAC Data is Confidential Information and subject to all requirements in Section 16 of these USAC Standard Terms and Conditions.

~~BB.~~Z. "USAC IT System(s)" means USAC's electronic computing and/or communications systems (including but not limited to various internet, intranet, extranet, email and voice mail).

~~CC.~~AA. "USAC Standard Terms and Conditions" means this document that provides the legal terms that govern this Contract.

~~DD.~~BB. "USF" means the Universal Service Fund.

2. TERM

The Initial Term is the period of time from the Effective Date (as defined in the cover sheet to this Contract) of the Contract to _____. After the conclusion of the Initial Term, USAC will have the right to extend the Contract Term by exercising up to _____ (__) one-year Optional Renewal Terms. USAC may exercise an Optional Renewal Term by written notice to Contractor within ~~ten~~ thirty (~~10~~30) days prior to expiration of the then current Initial Term or Optional Renewal Term.

3. ACCEPTANCE / REJECTION

Contractor shall only tender for acceptance Services and Deliverables that conform to the requirements of the Contract. USAC will, following Contractor's tender, inspect or test the Deliverables or Services and:

A. Accept the Services and Deliverables; or

B. Reject the Services and Deliverables and advise Contractor of the reasons for the rejection.

USAC will only accept Services or Deliverables that meet the acceptance criteria described in a statement of work or scope of work to the Contract. If the Service or Deliverable is Software or hardware intended for USAC IT Systems, USAC will require acceptance testing during an acceptance period that will be described in a statement of work or scope of work to the Contract.

USAC will reject any Service or Deliverable that does not conform to the acceptance criteria described in a statement of work or scope of work to the Contract. If rejected, Contractor must repair, correct, or replace

nonconforming Deliverables or re-perform nonconforming Services, at no increase in Contract price. If repair, correction, replacement, or re-performance by Contractor does not cure the defects within thirty (30) calendar days or if curing the defects is not possible, USAC may terminate for cause under Section 12 of these USAC Standard Terms and Conditions, and in addition to any other remedies, may reduce the Contract price to deduct amounts for the defective work.

Unless specified elsewhere in the Contract, title to items furnished under the Contract shall pass to USAC upon acceptance, regardless of when or where USAC takes possession.

4. ENTIRE CONTRACT / BINDING EFFECT

The Contract supersedes and replaces all prior or contemporaneous representations, dealings, understandings, or agreements, written or oral, regarding such subject matter. In the event of any conflict between these USAC Standard Terms and Conditions and any other document made part of the Contract, the USAC Standard Terms and Conditions shall govern. The Contract shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors and assignees.

5. MODIFICATIONS

The terms of the Contract, including these USAC Standard Terms and Conditions, shall not be modified other than in writing executed by both parties.

6. INVOICES

A. *Where to Submit Invoices.* Contractor shall submit all invoices in PDF format to accounting@usac.org for processing. For assistance on billing questions, Contractor may email the USAC Accounting team at accounting@usac.org. ~~*Where to Submit Invoices.* Contractor shall submit invoices through the UCSP method or via the SAN method. The UCSP method will require Contractor to register and create an account for the UCSP. An invitation link to the UCSP may be obtained by emailing CoupaHelp@usac.org. The SAN method will require Contractor to invoice USAC directly from the purchase order sent by USAC via email. For the SAN method, the USAC email will contain a notification with action buttons which will allow Contractor to create an invoice, add a comment, and acknowledge the receipt of the purchase order. For assistance on all Coupa related billing questions, Contractor may email CoupaHelp@usac.org. For assistance on all non-Coupa related billing questions, Contractor may email accounting@usac.org.~~

B. *Invoice Submittal Date.* Contractor may submit invoices for payment upon completion and USAC's acceptance of all of the work associated with a Contract or, if the period of performance of a Contract exceeds sixty (60) days, once every thirty (30) days, with the submission of the first invoice no earlier than thirty (30) days after issuance of the Contract.

C. *Content of Periodic Invoices.* If periodic invoices are submitted for a Contract, each invoice shall include only Services that have been completed and Deliverables that have been accepted as of the date of invoice submission and that have not been billed in a prior invoice.

Universal Service Administrative Co.

D. *Itemization of Invoices.* USAC may require Contractor to re-submit any invoice with a more detailed itemization of charges upon request.

7. FEES AND RATES INCLUSIVE OF ALL CHARGES AND TAXES

All fees and labor rates specified in the Contract include all charges for labeling, packing, packaging, loading, storage, inspection, insurance, profit, and applicable federal, state, or local sales, use, or excise taxes.

8. PAYMENT

Contractor shall be paid for Services performed on a fixed-price, service category rate basis using the service categories and fixed rates set forth in **Attachment 1**. USAC will pay invoices submitted in accordance with Section 6 of these USAC Standard Terms and Conditions within thirty (30) calendar days of receipt of invoice, provided the Services and/or Deliverables have been delivered and accepted by USAC.

Contractor will promptly credit to USAC any payment made to which Contractor is not entitled under these USAC Standard Terms and Conditions and refund to USAC any such payment for which there are not sufficient fees against which to credit the overpayment.

Under no circumstance will USAC be liable to pay Contractor any fees not invoiced within ninety (90) days after Contractor was first permitted to invoice USAC as described in Section 6 of these USAC Standard Terms and Conditions.

9. ASSIGNMENT, DELEGATION, AND SUBCONTRACTING

Contractor shall not assign, delegate, or subcontract all or any portion of the Contract without obtaining USAC's prior written consent. Consent must be obtained at least thirty (30) days prior to the proposed assignment, delegation, or subcontracting. USAC may require information and assurances that the proposed assignee, delegate, or subcontractor has the skills, capacity, qualifications, and financial strength to meet all of the obligations under the Contract. An assignment, delegation, or subcontract shall not release Contractor of the obligations under the Contract, and the assignee, delegate, or subcontractor shall be jointly and severally liable with Contractor. Contractor shall not enter into any subcontract with a company or entity that is debarred, suspended, or proposed for debarment or suspension by any federal executive agency unless USAC agrees with Contractor that there is a compelling reason to do so. Contractor shall review the SAM for suspension or debarment status of proposed subcontractors.

10. REPORTS

If any reports are required as part of this Contract, all such reports shall be accurate and timely and submitted in accordance with the due dates specified in this Contract. Should Contractor fail to submit any required reports or correct inaccurate reports, USAC reserves the right to delay payment of invoices until thirty (30) days after an accurate report is received and accepted.

Universal Service Administrative Co.

11. TERMINATION FOR CONVENIENCE

USAC may terminate the Contract for any reason or no reason upon one (1) day prior written notice to Contractor without any liability or obligation thereafter. Subject to the terms of the Contract, Contractor shall be paid for all time actually spent performing the Services required by the Contract up to date of termination, plus reasonable charges that USAC, in its sole discretion, agrees in writing have resulted directly from the termination.

12. TERMINATION FOR CAUSE

Either party may terminate the Contract for cause upon providing the other party with a written notice. Such notice will provide the other party with a ten (10) day cure period. Upon the expiration of the ten (10) day cure period (during which the defaulting party does not provide a sufficient cure), the non-defaulting party may immediately thereafter terminate the Contract, in whole or in part, if the defaulting party continues to fail to comply with any term or condition of the Contract or fails to provide the non-defaulting party, upon request, with adequate assurances of future performance. In the event of termination for cause, the non-defaulting party shall be entitled to any and all rights and remedies provided by law or equity. If it is determined that USAC improperly terminated the Contract for cause, such termination shall be deemed a termination for convenience. In the event of partial termination, the defaulting party shall continue to perform the portion of the Services not terminated.

13. STOP WORK ORDER

USAC may, in its sole discretion and without further obligation or liability, issue a stop work order at any time during the Contract Term. Upon receipt of a stop work notice, or upon receipt of a notice of termination (for cause or convenience), unless otherwise directed by USAC in writing, Contractor shall, on the stop work date identified in the stop work or termination notice: (a) stop work, and cause Contractor Staff to stop work, to the extent specified in said notice; and (b) subject to the prior written approval of USAC, transfer title and/or applicable licenses, as appropriate, to USAC and deliver to USAC, or as directed by USAC, all USAC Data, Confidential Information, Software, Deliverable, or any Derivative Work to any of the preceding, whether completed or in process, for the work stopped. In the event of a stop work order, all deadlines in the Contract shall be extended on a day for day basis from such date, plus reasonable additional time, as agreed upon between the parties, acting in good faith, to allow Contractor to reconstitute its staff and resume the work.

14. LIMITATION OF LIABILITY

Except in cases of gross negligence or willful misconduct, in no event shall USAC be liable for any consequential, special, incidental, indirect, or punitive damages arising under or relating to the performance of the Contract. USAC's entire cumulative liability from any causes whatsoever, and regardless of the form of action or actions, whether in contract, warranty, or tort (including negligence), arising under the Contract shall in no event exceed the aggregate amount paid by USAC to Contractor in the year preceding the most

recent of such claims. All exclusions or limitations of damages contained in the Contract, including, without limitation, the provisions of this Section, shall survive expiration or termination of the Contract.

15. INDEMNITY

Contractor shall indemnify, hold harmless, and defend USAC and its directors, officers, employees, and agents against any and all demands, claims and liability, costs and expenses (including attorney's fees and court costs), directly or indirectly related to: (a) any claims or demands for actual or alleged direct or contributory infringement of, or inducement to infringe, or misappropriation of, any intellectual property, including, but not limited to, trade secret, patent, trademark, service mark, or copyright, arising out of or related to Contractor's performance of the Contract; (b) any claims or demands for personal injuries, death, or damage to tangible personal or real property to the extent caused by the intentional, reckless, or negligent acts or omissions of Contractor or Contractor Staff in connection with this Contract; and (c) any claims or demands of any nature whatsoever to the extent caused by Contractor's breach of any confidentiality, security, or privacy obligations set forth in these USAC Standard Terms and Conditions by Contractor or Contractor Staff; (d) Contractor's unauthorized use of USAC Software, USAC IT Systems, or USAC Data; (e) any breach of applicable law as described in Section 27 of these USAC Standard Terms and Conditions by Contractor or Contractor Staff; or (f) the negligent, reckless, illegal, or intentional acts or omissions of Contractor or Contractor Staff in connection with the performance of the Services.

16. CONFIDENTIAL INFORMATION

A. *Confidential Information*. Confidential Information includes, but is not limited to, USAC Data, materials, or communications in any form or format, whether tangible or intangible, spoken or written (regardless of media) that contains, reflects, or is derived from or based upon, or is related to:

1. Management, business, procurement, or financial information of either party, the FCC, or a USF stakeholder, including proprietary or commercial information and trade secrets that have not previously been publicly disclosed;

2. Information regarding USAC's processes and procedures (including, but not limited to, program operational information, information regarding USAC's administration of its programs, and information regarding USAC's processing of applications for program support);

3. Information concerning USAC's relationships with other vendors or contractors, the FCC, USF Stakeholders, or financial institutions;

4. Information marked to indicate disclosure limitations such as "Confidential," "Confidential Information," "Contains PII," "Highly Confidential – Restricted," "Administrative Hold," "proprietary," "privileged," "not for public disclosure," "work product," etc.;



5. Information compiled, prepared, or developed by Contractor in the performance of the Contract;

6. PII [defined in the USAC Standard Terms and Conditions Privacy and Security Addendum.]; and

7. Information that Recipient knows or reasonably should have known is confidential, proprietary, or privileged.

B. *Non-Disclosure/Use/Irreparable Harm*. It is anticipated that a Discloser may disclose, or has disclosed, Confidential Information to the Recipient. At all times during the term of the Contract and thereafter, the Recipient shall maintain the confidentiality of all Confidential Information and prevent its unauthorized disclosure, publication, dissemination, destruction, loss, or alteration. Recipient shall only use Confidential Information for a legitimate business purpose of USAC and in the performance of the Contract. Recipient acknowledges that the misappropriation, unauthorized use, or disclosure of Confidential Information would cause irreparable harm to the Disclosing Party and could cause irreparable harm to the integrity of the USF programs.

C. *Sub-Recipient Access to Confidential Information*. Recipient shall not disclose Confidential Information to a Sub-Recipient unless absolutely necessary for a Recipient's or Sub-Recipient's performance of the Contract, and if necessary, shall only disclose the Confidential Information necessary for Sub-Recipient's performance of its duties. As a pre-condition to access to Confidential Information, Recipient shall require Sub-Recipients, including Contractor Staff, to sign a non-disclosure or confidentiality agreement containing terms no less restrictive than those set forth herein. Discloser may enforce such agreements, if necessary, as a third-party beneficiary.

D. *Contractor Enforcement of Confidentiality Agreement*. Contractor must report, and describe in detail, any breach or suspected breach of the non-disclosure requirements set forth above to the USAC General Counsel within one (1) hour upon becoming aware of the breach. Contractor will follow-up with the USAC Privacy Officer and provide information on when and how the breach occurred, who was involved, and what has been done to recover the Confidential Information.

E. *Exclusions*. If requested to disclose Confidential Information by an authorized governmental or judicial body, Recipient must promptly notify Discloser of the request, and to the extent that it may legally do so, Recipient must refrain from disclosure of the Confidential Information until Discloser has had sufficient time to take any action as it deems appropriate to protect the Confidential Information. In the event Confidential Information of USAC is requested, Recipient must immediately notify USAC, with a copy to USAC's General Counsel, of the request. Neither Contractor nor Contractor Staff shall issue any public statement relating to or in any way disclosing any aspect of the Contract without the prior written consent of USAC. Notwithstanding anything herein to the contrary, USAC may, without notice to Contractor, provide the Contract, including Contractor's proposal information, and any information or USAC Data delivered, prepared, or developed by Contractor in the performance of the Contract to the FCC or other governmental or judicial body, and may publicly disclose basic information regarding the

Universal Service Administrative Co.

Contract, e.g., name of Contractor, price, basis for selection, description of Services/Deliverables and any provisions necessary for USAC to justify actions taken with respect to the Contract.

17. RETURN OR DESTRUCTION OF USAC DATA

A. *Return or Destruction of USAC Data.* Except as provided in Section 17.B of these USAC Standard Terms and Conditions, and promptly upon the expiration or termination of the Contract (or such earlier time as USAC may direct), Contractor shall, at the direction of USAC, and at no additional cost to USAC, return or destroy all USAC Data, including all copies thereof, in the possession or under the control of Contractor or Contractor Staff. If USAC directs that Contractor destroy any USAC Data, then, at USAC's request, Contractor shall provide USAC with an executed certificate in writing stating that all such USAC Data was destroyed.

B. *Acknowledgement of Data Inclusion in Federal System of Record.* Contractor acknowledges and agrees that certain USAC Data may be included in a federal system of record and is subject to record retention schedules set forth by the National Archives and Record Administration and to USAC's records retention policy. Upon expiration or termination of the Contract, information subject to the National Archives and Record Administration's schedules or to USAC's records retention policy shall not be destroyed by Contractor without the written consent of USAC. Contractor will work with USAC in good faith to promptly return all such USAC Data to USAC.

C. *No Withholding of USAC Data*. Contractor shall not withhold any USAC Data as a means of resolving any dispute. To the extent that there is a dispute between Contractor and USAC, Contractor may make a copy of such USAC Data as is necessary and relevant to resolution of the dispute. Any such copies shall promptly be destroyed upon resolution of the dispute.

D. *Destruction of Hard Copies.* If Contractor destroys hard copies of USAC Data, Contractor must do so by burning, pulping, shredding, macerating, or other means if authorized by USAC in writing.

E. *Destruction of Electronic Copies.* If Contractor destroys electronic copies in computer memory or any other type of media, destruction must be done pursuant to guidelines in NIST SP 800-88 Rev. 2 or the most current revision. ["NIST" is defined in the USAC Standard Terms and Conditions Privacy and Security Addendum.]

F. *No Other Use.* USAC Data is provided to Contractor solely for the purpose of rendering the Services, and USAC Data or any part thereof shall not be sold, assigned, leased, or otherwise transferred to any third party by Contractor (except as required to perform the Services or as otherwise authorized in the Contract), commingled with non-USAC Data, modified, decompiled, reverse engineered, or commercially exploited by or on behalf of Contractor, Contractor Staff, or any third party.

18. PROPRIETARY RIGHTS

Universal Service Administrative Co.

Contractor agrees that all USAC Data, Software, Deliverables, and all Derivative Works thereof are USAC property and shall be deemed USAC Data and are works made-for-hire for USAC within the meaning of the copyright laws of the United States. In the event that any of the aforementioned are not considered works made-for-hire for USAC within the meaning of the copyright laws of the United States, Contractor shall and hereby does irrevocably grant, assign, transfer and set over unto USAC in perpetuity all worldwide rights, title, and interest of any kind, nature, or description it has or may have in the future in and to such materials, and Contractor shall not be entitled to make any use of such materials beyond what may be described in this Contract. Contractor hereby waives, and shall secure a waiver from Contractor Staff any moral rights in such assigned materials, such as the right to be named as author, the right to modify, the right to prevent mutilation, and the right to prevent commercial exploitation. Accordingly, USAC shall be the sole and exclusive owner for all purposes for the worldwide use, distribution, exhibition, advertising and exploitation of such materials or any part of them in any way and in all media and by all means.

USAC may assign to the FCC any intellectual property rights USAC may have to any USAC Data, Software, Deliverables, and all Derivative Works thereof without notice to, or prior consent of, Contractor.

Nothing in this Contract shall be deemed to imply the grant of a license in or transfer of ownership or other rights in the USAC Data, Software, Deliverables, or Derivative Works thereof, and Contractor acknowledges and agrees that it does not acquire any of the same, except to provide Services to USAC as expressly set forth in this Contract.

Contractor shall not, without the prior written permission of USAC, incorporate any USAC Data, Software, Deliverable, or Derivative Work thereof delivered under the Contract not first produced in the performance of the Contract unless Contractor: (a) identifies the USAC Data, Software, Deliverable, or Derivative Work thereof; and (b) grants to USAC, or acquires on USAC's behalf, a perpetual, worldwide, royalty-free, non-exclusive, transferable license to use and modify such USAC Data, Software, Deliverable, or Derivative Work thereof in any way.

19. RESPONSIBILITY FOR CONTRACTOR STAFF

Contractor Staff working on USAC premises are required to sign and agree to the terms of a Visitor Form provided by USAC. Contractor is responsible for any actions of Contractor Staff, including any actions that violate the law, are negligent, or that constitute a breach of the Visitor Form and/or the Contract.

Contractor shall conduct background checks on Contractor Staff and provide evidence of the background checks to USAC upon request.

20. KEY PERSONNEL

Universal Service Administrative Co.

USAC may specify which Contractor employees are Key Personnel under the Contract. Key Personnel assigned to the Contract must remain in their respective positions throughout the Contract Term. USAC may terminate all or a part of the Contract if Contractor changes the position, role, or time commitment of Key Personnel, or removes Key Personnel from the Contract, without USAC's prior written approval. USAC may grant approval for changes in staffing of Key Personnel if it determines in its sole discretion, that:

A. changes to, or removal of, Key Personnel is necessary due to extraordinary circumstances (e.g., a Key Personnel's illness, death, termination of employment, or absence due to family leave), and

B. Contractor has resources (e.g., replacement personnel) with the requisite skills, qualifications, and availability to perform the role and duties of the outgoing personnel.

Replacement personnel are considered Key Personnel and this Section shall apply to their placement on and removal from the Contract.

21. SHIPMENT/DELIVERY

Terms of any shipping are F.O.B. USAC's delivery location unless otherwise noted in the Contract. All goods, products items, materials, etc. purchased hereunder must be packed and packaged to ensure safe delivery in accordance with recognized industry-standard commercial practices. If, in order to comply with the applicable delivery date, Contractor must ship by a more expensive means than that specified in the Contract, Contractor shall bear the increased transportation costs resulting therefrom unless the necessity for such shipment change has been caused by USAC. If any Deliverable is not delivered by the date specified herein, USAC reserves the right, without liability, to cancel the Contract as to any Deliverable not yet shipped or tendered, and to purchase substitute materials and to charge Contractor for any loss incurred. Contractor shall notify USAC in writing promptly of any actual or potential delays (however caused) which may delay the timely performance of this Contract. If Contractor is unable to complete performance at the time specified for delivery hereunder, by reason of causes beyond Contractor's reasonable control, USAC may elect to take delivery of materials in an unfinished state and to pay such proportion of the Contract price as the work then completed bears to the total work hereunder and to terminate this Contract without liability as to the balance of the materials covered hereunder.

22. INSURANCE

At its own expense, Contractor shall maintain sufficient insurance in amounts required by law or appropriate for the industry, whichever is greater, to protect and compensate USAC from all claims, risks, and damages/injuries that may arise under the Contract, including, as appropriate, worker's compensation, employer's liability, commercial general liability, commercial crime coverage, automobile liability, professional liability, cyber liability and artificial intelligence (AI)-related cyber liability (which may be included in some professional liability coverage), and excess / umbrella insurance. Upon USAC's request,

Universal Service Administrative Co.

Contractor shall name USAC as an additional insured to those insurance policies that allow it. Upon USAC's request, Contractor shall cause its insurers to waive their rights of subrogation against USAC. Contractor shall produce evidence of such insurance upon request by USAC. If the insurance coverage is provided on a claims-made basis, then it must be maintained for a period of not less than three (3) years after acceptance of the Deliverables and/or Services provided in connection with this Contract. Contractor shall provide written notice thirty (30) days prior to USAC in the event of cancellation of or material change in the policy.

Contractor shall be liable to USAC for all damages incurred by USAC as a result of Contractor's failure to maintain the required coverages with respect to its subcontractors, or Contractor's failure to require its subcontractors to maintain the coverages required herein.

23. CONFLICTS OF INTEREST

It is essential that any Contractor providing Services or Deliverables in support of USAC's administration of the USF maintain the same neutrality as USAC, both in fact and in appearance, and avoid any organizational or personal conflict of interest, or even the appearance of a conflict of interest. For example, to the extent that Contractor, or any of its principals, has client, membership, financial and/or any other material affiliation with entities that participate in the federal USF in any respect, there may be actual, potential and/or apparent conflict(s) of interest. Contractor shall maintain written standards of conduct covering conflicts of interest and provide a copy to USAC upon USAC's request. Contractor shall promptly notify USAC's General Counsel in writing of any actual or potential conflicts of interest involving Contractor, or any circumstances that give rise to the appearance of a conflict of interest, and the means by which Contractor proposes to avoid, neutralize, or mitigate such conflicts. Contractor shall also notify USAC promptly of any conflicts Contractor has with USAC vendors. Failure to provide adequate means to avoid, neutralize or remediate any conflict of interest may be the basis for termination of the Contract. By its execution hereof, Contractor represents and certifies that it has not paid or promised to pay a gratuity, or offered current or future employment or consultancy, to any USAC or government employee in connection with the award of this Contract. In order to maintain the absence of an actual or apparent conflict of interest as described herein, Contractor must not advocate any policy positions with respect to the USF programs or the USF during the term of the Contract. Neither Contractor nor its subcontractors shall issue any public statement relating to or in any way disclosing any aspect of the Contract without the prior written consent of USAC.

24. WAIVER

Any waiver of any provision of this Contract must be in writing and signed by the parties hereto. Any waiver by either party of a breach of any provision of this Contract by the other party shall not operate or be construed as a waiver of any subsequent breach by the other party.

25. SEVERABILITY

The invalidity or unenforceability of any provisions of the Contract shall not affect the validity or enforceability of any other provision of the Contract, which shall remain in full force and effect. The parties further agree to negotiate replacement provisions for any unenforceable term that are as close as possible to the original term, and to change such original term only to the extent necessary to render the term valid and enforceable.

26. CHOICE OF LAW / CONSENT TO JURISDICTION

The Contract shall be governed by and construed in accordance with the laws of the District of Columbia without regard to any otherwise applicable principle of conflicts of laws. Contractor agrees that all actions or proceedings arising in connection with the Contract shall be litigated exclusively in Courts. This choice of venue is intended to be mandatory and the parties waive any right to assert forum non conveniens or similar objection to venue. Each party hereby consents to in personam jurisdiction in the Courts. Contractor must submit all claims or other disputes to the procurement specialist and USAC General Counsel for informal resolution prior to initiating any action in the Courts and must work with USAC in good faith to resolve any disputed issues. If any disputed issue by Contractor is not resolved after thirty (30) calendar days of good faith attempts to resolve it, Contractor may instigate legal proceedings. A dispute over payment or performance, whether informal or in the Courts, shall not relieve Contractor of its obligation to continue performance of the Contract and Contractor shall proceed diligently with performance during any dispute over performance or payment.

27. USAC AND APPLICABLE LAWS

USAC is not a federal agency, a government corporation, a government controlled corporation, or any other establishment in the Executive Branch of the United States government. USAC is not a contractor to the federal government and the Contract is not a subcontract under a federal prime contract. USAC conducts its procurements in accordance with the terms of a Memorandum of Understanding with the FCC, which requires USAC and its Contractors to adhere to the Procurement Regulations. Contractor shall comply with the Procurement Regulations and all applicable federal, state and local laws, executive orders, rules, regulations, declarations, decrees, directives, legislative enactments, orders, ordinances, common law, guidance, and other binding restriction or requirement of or by any governmental authority related to the Services or Contractor's performance of its obligations under this Contract, and includes without limitation FCC Orders; the rules, regulations and policies of the FCC; the Privacy Act of 1974; and the laws and guidelines named in the USAC Standard Terms and Conditions Privacy and Security Addendum.

28. RIGHTS IN THE EVENT OF BANKRUPTCY

All licenses or other rights granted under or pursuant to the Contract are, and shall otherwise be deemed to be, for purposes of Section 365(n) of the Code, licenses of rights to "intellectual property" as defined in the Code. The parties agree that USAC, as licensee of such rights under Contractor, shall retain and may fully exercise all of its rights and elections under the Code. The parties further agree that, in the event of the commencement of bankruptcy proceedings by or against Contractor under the Code, USAC shall be entitled

to retain all of its rights under the Contract and shall not, as a result of such proceedings, forfeit its rights to any USAC Data, Software, Deliverable, or any Derivative Work thereof.

29. NON EXCLUSIVITY

Except as may be set forth in the Contract, nothing herein shall be deemed to preclude USAC from retaining the services of other persons or entities undertaking the same or similar functions as those undertaken by Contractor hereunder or from independently developing or acquiring goods or services that are similar to, or competitive with, the goods or services, as the case may be, contemplated under the Contract.

30. INDEPENDENT CONTRACTOR

Contractor acknowledges and agrees that it is an independent contractor to USAC and Contractor Staff are not employees of USAC. USAC will not withhold or contribute to Social Security, workers' compensation, federal or state income tax, unemployment compensation or other employee benefit programs on behalf of Contractor or Contractor Staff. Contractor shall indemnify and hold USAC harmless against any and all loss, liability, cost, and expense (including attorneys' fees) incurred by USAC as a result of USAC not withholding or making such payments. Neither Contractor nor any of Contractor Staff are entitled to participate in any of the employee benefit plans of, or otherwise obtain any employee benefits from, USAC. USAC has no obligation to make any payments to Contractor Staff. Contractor shall not hold herself/himself out as an employee of USAC and Contractor has no authority to bind USAC except as expressly permitted hereunder.

31. TEMPORARY EXTENSION OF SERVICES

USAC may require continued performance of any Services within the limits and at the rates specified in the Contract. Except as may be set forth in the Contract, USAC may extend the Services more than once, but the total extension of performance hereunder shall not exceed six (6) months. USAC may exercise an option to extend by written notice to Contractor within ten (10) days prior to expiration of the then current Initial Term or Optional Renewal Term.

32. NOTICES

All notices, consents, approvals or other communications required or authorized by the Contract shall be given in writing and shall be:

A. personally delivered,
B. mailed by registered or certified mail (return receipt requested) postage prepaid,
C. sent by overnight delivery service (with a receipt for delivery), or
D. sent by electronic mail with a confirmation of receipt returned by recipient's electronic mail server to such party at the following address:

If to USAC:
Chief Administrative Officer, Universal Service Administrative Company

Universal Service Administrative Co.

700 12th Street, NW, Suite 900
Washington, DC 20005
Email: To the designated USAC Contract Officer for this procurement, with a copy to usacprocurement@usac.org.

With a copy to:

General Counsel, Universal Service Administrative Company
700 12th Street, NW, Suite 900
Washington, DC 20005
Email: OGCContracts@usac.org

If to Contractor: To the address or email set forth in Contractor's proposal in response to the Solicitation.

33. SURVIVAL

All provisions that logically should survive the expiration or termination of the Contract shall remain in full force and effect after expiration or early termination of the term of the Contract. Without limitation, all provisions relating to return of USAC Data, confidentiality obligations, proprietary rights, and indemnification obligations shall survive the expiration or termination of the Contract.

34. FORCE MAJEURE

Neither party to this Contract is liable for any delays or failures in its performance hereunder resulting from circumstances or causes beyond its reasonable control, including, without limitation, force majeure acts of God (but excluding weather conditions regardless of severity), fires, accidents, epidemics, pandemics, riots, strikes, acts or threatened acts of terrorism, war or other violence, or any law, order or requirement of any governmental agency or authority (but excluding orders or requirements pertaining to tax liability). Upon the occurrence of a force majeure event, the non-performing party shall provide immediate notice to the other party and will be excused from any further performance of its obligations effected by the force majeure event for so long as the event continues and such party continues to use commercially reasonable efforts to resume performance as soon as reasonably practicable, and continues to take reasonable steps to mitigate the impact on the other party. If such non-performance continues for more than ten (10) days, then the other party may terminate this Contract with at least one (1) day prior written notice to the other party. In the event that the force majeure event is a law, order, or requirement made by a government agency or authority related to USAC and the purposes of this Contract, USAC may immediately terminate this Contract without penalty upon written notification to Contractor.

35. EXECUTION / AUTHORITY

The Contract may be executed by the parties hereto on any number of separate counterparts and counterparts taken together shall be deemed to constitute one and the same instrument. A signature sent via facsimile or portable document format (PDF) shall be as effective as if it was an original signature. Each person signing

the Contract represents and warrants that they are duly authorized to sign the Contract on behalf of their respective party and that their signature binds their party to all provisions hereof.

36. NATIONAL SECURITY SUPPLY CHAIN REQUIREMENTS

A. *Definitions.* For purposes of this Section, the following terms are defined as stated below:

1. "Covered Company" is defined as an entity, including its parents, affiliates, or subsidiaries, finally designated by the Public Safety and Homeland Security Bureau of the FCC as posing a national security threat to the integrity of communications networks or the communications supply chain.
2. "Covered Equipment or Services" is defined as equipment or services included on the FCC-issued Covered List that pose a national security threat to the integrity of the communications supply chain.
3. "Covered List" is a list of covered communications equipment and services that pose an unacceptable risk to the national security of the United States. The FCC may update the list at any time. The list can be found at fcc.gov/supply chain/covered list.
4. "Reasonable Inquiry" is defined as an inquiry designed to uncover information about the identity of the producer or provider of equipment and services that has been purchased, obtained, maintained, or otherwise supported by funds from USAC under this Contract.

~~B.~~A. *Prohibition*. Contractor will ensure that no funds from USAC or other federal subsidies under this Contract will be used to purchase, obtain, maintain, or otherwise support any equipment or services produced or provided by a Covered Company. Contractor must also ensure that no funds administered by USAC or the FCC under this Contract will be used to purchase, obtain, maintain, or otherwise support Covered Equipment or Services placed on the Covered List. These prohibitions extend to any subcontractors that provides Services under the Contract. Contractor is responsible for notifying any subcontractors it engages under this Contract of this prohibition.

~~C.~~B. *Monitoring*. Contractor must actively monitor what entities have been finally designated by the FCC as a Covered Company and what equipment and services the FCC defines as Covered Equipment or Services and places on the Covered List. Contractor must actively monitor to ensure that no funds from USAC or other federal subsidies are used to purchase, obtain, maintain, or otherwise support any equipment or services produced or provided by a Covered Company from Contactor or any subcontractor it engages under the Contract. Contractor must also ensure that no funds administered by USAC or other federal subsidies are used to purchase, obtain, maintain, or otherwise support any Covered Equipment or Services that the FCC has placed on the Covered List from Contractor or any subcontractor it engages under the Contract. If Contractor finds that they have violated any or all of these prohibitions, then Contractor shall immediately notify USAC. In Contractor's notification to USAC, Contractor shall provide the same information required for non-compliance in Section 36.D of

these USAC Standard Terms and Conditions. Any such notification must have audit ready supporting evidence.

~~D.~~C. *Annual Inquiry & Certifications*. Contractor will conduct a Reasonable Inquiry upon execution of this Contract and no later than December 31 of each calendar year that the Contract is in effect. If Contractor, or any applicable subcontractor, is not in compliance with Section 36.B. of these USAC Standard Terms and Conditions, Contractor shall inform USAC and provide the following information in the certification:

(i) If for equipment produced or provided by a Covered Company or equipment on the Covered List:
   a. The Covered Company that produced the equipment (include entity name, unique entity identifier, CAGE code, and whether the Covered Company was the original equipment manufacturer ("OEM") or a distributor, if known);
   b. A description of all equipment (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and
   c. Explanation of why USAC funds purchased, obtained, maintained, or otherwise supported the equipment and a plan to remove and replace such equipment as expeditiously as possible.

(ii) If for services produced or provided by a Covered Company or services on the Covered List:
   a. If the service is related to item maintenance: A description of all such services provided (include on the item being maintained: brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable);
   b. If the service is not associated with maintenance, the product service code of the service being provided; and
   c. Explanation of the why USAC funds purchased, obtained, maintained, or otherwise supported the services and a plan to remove and replace such service as expeditiously as possible.

At USAC's discretion, and at any time during the performance of this contract, USAC may require the Contractor to certify it, and all applicable subcontractors, are in compliance with Section 36.B of these USAC Standard Terms and Conditions. Contractor shall state in the certification that no funds from USAC have been used to purchase, obtain, maintain, or otherwise support any equipment or services produced by a Covered Company or Covered Equipment or Services on the Covered List.
Contractor shall retain supporting evidence for all certifications.

37. PROHIBITION ON A BYTEDANCE COVERED APPLICATION

Universal Service Administrative Co.

1. *Definitions.* For purposes of this Section, the following terms are defined as stated below:

   1. *"Covered Application"* means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

   2. *"Information Technology"* means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by USAC, if the equipment is used by USAC directly or is used by Contractor under this Contract with USAC that requires the use—

      a. Of that equipment; or
      b. Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

      The definition of "*Information Technology*" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

      The definition of "*Information Technology*" does not include any equipment acquired by a Contractor incidental to this Contract.

2. *Prohibition*. Contractor is prohibited from having or using a Covered Application on any Information Technology owned or managed by USAC, or on any Information Technology used or provided by Contractor under this Contract, including equipment provided by Contractor Staff.

3. *Subcontracts*. Contractor shall insert the substance of this clause, including this subsection C, in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.

38. ADDED SERVICES

USAC may at any time submit a request that Contractor perform any Added Services. Before Contractor performs any Added Services, USAC and Contractor must execute an amendment to this Contract that, at a minimum, will provide: (a) a detailed description of the services, functions and responsibilities of the Added Service; (b) a schedule for commencement and completion of the Added Services; (c) a detailed breakdown of Contractor's fees for the Added Services; (d) a description of any new staffing and equipment to be provided by Contractor to perform the Added Services; and (e) such other information as may be requested by USAC.

Universal Service Administrative Co.

39. PRIVACY AND SECURITY ADDENDUM

Contractor must comply with the privacy and security requirements and obligations found in the USAC Standard Terms and Conditions Privacy and Security Addendum.

40. SECTION 508 STANDARDS

Compliance with Section 508. Contractor shall ensure that Services provided under the Contract comply with the applicable electronic and information technology accessibility standards established in 36 C.F.R. Part 1194, which implements Section 508 of the Rehabilitation Act, 29 U.S.C. § 794d.

TDD/TTY Users. Contractor shall ensure that TDD/TTY users are offered similar levels of service that are received by telephone users supported by the Contract. Contractor shall also ensure that the Services provided under the Contract comply with the applicable requirements of 18 U.S.C. § 2511 and any applicable state wiretapping laws.

Universal Service Administrative Co.

USAC STANDARD TERMS AND CONDITIONS

PRIVACY AND SECURITY ADDENDUM

This is the USAC Standard Terms and Conditions Privacy and Security Addendum to, and hereby incorporates, the USAC Standard Terms and Conditions between Universal Service Administrative Company ("USAC") and _____. ("Contractor"), dated as of INSERT DATE (the "USAC Standard Terms and Conditions"). Capitalized terms used but not defined herein shall have the meanings ascribed to such terms in the Contract.

1. DEFINITIONS

"Artificial Intelligence" or "AI"	An engineered or machine-based automated system, software, algorithm, or technology – whether or not described by Contractor as "artificial intelligence" – that can, for a given set of explicit or implicit objectives, perform tasks and generate outputs consisting of reasoning, learning, predictions, decision-making, recommendations, or decisions influencing real or virtual environments. This includes, but is not limited to, machine learning models, natural language processing systems, computer visions systems, generative AI and any successor or related technologies designed to operate with varying levels of autonomy.~~A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.~~
"Authority to Operate" or "ATO"	The official management decision given by a USAC official or officials to authorize operation of an information system and to explicitly accept the risk to USAC operations (including mission, functions, image, or reputation), USAC assets, individuals, and other organizations based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.
"Contractor IT"	Any information technology device, software, hardware, equipment, system, and/or any IaaS, PaaS, or SaaS provided by a CSP that is owned or managed by the Contractor, its agents, or subcontractors.
"Cloud Protocols"	A comprehensive information security program governing standard technical configurations, platforms, or sets of procedures used in connection with the Services operated in cloud infrastructure environments.
"Cloud Service Offering"	A service from a cloud service provider. FedRAMP categorizes Cloud Service Offerings as one of the following: IaaS, PaaS, or SaaS.
"Cloud Service Provider" or "CSP"	A provider of IT infrastructure, products, or SaaS to be acquired by a user of IT services.

"COTS"	Commercial off-the-shelf Software, which is Software, hardware, and information technology products that (1) already exist, (2) are available from commercial sources, (3) are ready-made, and (4) are available for purchase by the general public.
"Cybersecurity/Data Breach"	A successful incident in which sensitive, confidential, or otherwise protected system/data has been accessed and/or disclosed in an unauthorized fashion. For example, a brute force attack against a protected system, attempting to guess multiple usernames and passwords, is a Cybersecurity Incident, but cannot be defined as a Cybersecurity/Data Breach unless the attacker succeeded in guessing a password. If a Cybersecurity Incident grants the attacker access to protected systems, it may qualify as a Cybersecurity/Data Breach. If the attacker obtained access to USAC Data, it is a Cybersecurity/Data Breach. Not every Cybersecurity Incident is a Cybersecurity/Data Breach, Privacy Incident, or a Privacy Breach. Most Cybersecurity Incidents do not result in actual Cybersecurity/Data Breach. Examples of Cybersecurity/Data Breaches may include, but are not limited to: • Bringing down the USAC.org website (for example, through a Denial of Service (DoS) Attack. • Employees cause ransomware to be installed and encrypt computer or entire network (Phishing Attack, DoS Attack) • Attackers obtain USAC Data through unauthorized access. • Unencrypted USAC Data being disseminated through peer-to-peer file sharing service.
"Cybersecurity Incident"	An event that attempts to or successfully compromises the integrity, confidentiality, and/or availability of an information asset or USAC Data. A Cybersecurity Incident could be either intentional or accidental in nature. Cybersecurity incidents hereafter may be referred to as a "Cyber Incident" or "Incident".

"Data at Rest"	State of data while it is on the device that stores it, or data that has reached a destination and is not being accessed or used. This term is primarily used in the context of data encryption. It typically refers to stored data and excludes data that is moving across a network or is temporarily in computer memory waiting to be read or updated. It does not include data in use while it is being processed, accessed, or read where it must be decrypted to be used.
"Data in Transit"	Data transmitted via email, web, collaborative work applications, instant messaging, or any type of private or public communication channel. This term is primarily used in the context of data encryption. It includes all data moving between systems or devices on networks. It does not include data in use while it is being processed, accessed, or read where it must be decrypted to be used.
"Data Leakage"	The inadvertent exposure of data beyond its controlled environment or intended usage, such as a lost or stolen laptop, an employee storing files using an Internet storage application, or an employee saving files on a USB drive to take home.
"Data Loss"	The exposure of proprietary, sensitive, or classified information through either Data Theft or Data Leakage. This includes the intentional or unintentional destruction of information, caused by people and or processes from within or outside of an organization. In a Cybersecurity/Data Breach or Privacy Breach the data is compromised, but Data Loss further describes damage to the integrity, completeness, or control of the data.
"Data Safeguards"	Protections that safeguard USAC Data against destruction, loss, damage, corruption, alteration, loss of integrity, commingling, or unauthorized access or Processing.
"Data Security Laws"	FISMA, 44 U.S.C. § 3541, et seq., the Privacy Act as amended (as may be applicable), and NIST SP 800-53 Rev 5. PII protections in accordance with all federal and USAC requirements, including, but not limited to, OMB Memoranda M-17-12 and guidance from NIST including, but not limited to, NIST SP 800-53 Rev 5 and NIST SP 800-61 Rev 2 (or most current version), and FIPS 140-3. Any federally mandated information security and privacy requirements not described herein.
"Data Theft"	The deliberate or intentional act of stealing information such that controlled data is intentionally stolen or exposed, such as in cases of espionage or employee disgruntlement.
"Event"	An exception to the normal operation of IT infrastructure, systems, services, or privacy. Not all Events become a Cybersecurity Incident or Privacy Incident. Cybersecurity Incidents and Privacy Incidents are Events which can represent a threat, an attack, or a breach.

"Exfiltration"	The unauthorized transfer of information from USAC IT Systems.
"FedRAMP-Authorized," or "FedRAMP Authorization"	A term used to designate a Cloud Service Offering from a CSP that satisfies the security assessment, authorization, and continuous monitoring requirements of the Federal Risk and Authorization Management Program ("FedRAMP"), a US government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies; see FedRAMP.gov.
"FIPS"	Federal Information Processing Standards. FIPS are standards and guidelines for computer systems that are developed by NIST in accordance with FISMA and approved by the Secretary of Commerce. These standards and guidelines are developed when there are no acceptable industry standards or solutions for a particular requirement.
"FISMA"	The Federal Information Security Management Act, 44 U.S.C. §3541, *et seq*., as amended by the Federal Information Security Modernization Act of 2014, and their implementing and successor regulations.
"IaaS"	Infrastructure as a service.
"Malicious Code" or "Malware"	Any software, hardware, firmware, program, routine, protocol, script, code, command, logic, or other feature that performs an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system and that is: (a) designed to (i) disrupt, disable, deactivate, interfere with, or otherwise compromise USAC IT Systems, or (ii) access, modify, disclose, transmit, or delete PII, Confidential Information, or USAC Data; or (b) either inadvertently or upon the occurrence of a certain event, compromises the confidentiality, integrity, privacy, security, or availability of PII, Confidential Information, USAC Data, or USAC IT Systems. Examples of Malicious Code include, but are not limited to, viruses, worms, bugs, ransomware, spyware, bots, backdoors, devices, root kits, and Trojan Horses. For purposes of this definition, "root kits" are a set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

"Malicious Cyber Activity"	Any activity, other than those activities authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information systems, communications systems, networks, or physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
"Multifactor Authentication"	A type of authentication using two or more factors to achieve verification of the identity of a user, process, or device as a prerequisite to allowing access to an information system. A user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism. Factors include, but are not limited to: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); and/or (iii) something you are (e.g., biometric).
"NIST" and "NIST SP"	NIST means the National Institute of Standards and Technology, part of the U.S. Department of Commerce. NIST SP means a special publication published by NIST.
"OMB"	Office of Management and Budget.
"PaaS"	Platform as a service.
"Personally Identifiable Information" or "PII"	Personally Identifiable Information (PII) is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII include name, address, telephone number, date and place of birth, mother's maiden name, biometric records, social security number, etc.
"PIN"	Personal Identification Number
"Privacy Breach"	A breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to PII. When PII is involved in a Cybersecurity/Data Breach it then becomes a Privacy Breach.
"Privacy Incident"	An unauthorized use or disclosure of confidential, sensitive, or regulated data, like USAC Data, PII, or confidential commercial information. For example, an unauthorized user gains access to a system containing PII and exfiltrates the PII.

"Process" or "Processing"	Any operation or set of operations that is performed using USAC Data, whether or not by automatic means, including, but not limited to, collection, retention, logging, generation, transformation, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, destruction, transfer, or disposal.
"Risk Management Framework" or "RMF"	A seven (7) step process that any organization can use to manage information security and privacy risk for organizations and systems and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of FISMA.
"SaaS"	Software as a service.

2. SECURITY PROVISIONS

2.1. Data Security Laws Compliance. Contractor shall comply with the Data Security Laws. For any Contractor IT using a Cloud Service Offering that ~~accesses,~~accesses stores, or otherwise processes USAC Data, and/or PII, Contractor shall provide documentation and proof of FedRAMP Authorization for use at a moderate risk before any such cloud-based Service may be used. USAC reserves the right to inspect the Authority to Operate, or the complete package of documents for any Cloud Service Offering with agency accreditation.

2.2. Contractor Compliance Generally. Throughout the Contract Term, Contractor shall comply with: (i) USAC's information privacy and IT security policies; and (ii) the prevailing standards of care and best practices regarding information privacy and IT security to the extent they meet or exceed the requirements of the Data Security Laws, the aforementioned USAC policies, or the obligations set forth in this Privacy and Security Addendum or the USAC Standard Terms and Conditions.

2.3. Contractor Duties Prior to Delivering Services. Prior to delivering the Services or enabling data-sharing or interoperability of any kind with USAC IT Systems, Contractor shall: (i) demonstrate Contractor system is compliant with FISMA and NIST SP 800-53 Rev. 5 and has received an Authority to Operate by the Contractor's authorizing official after following the steps laid out in the NIST risk management framework by providing evidence thereof; (ii) work with USAC to document, establish and enable the effective and secure integration of any gateways or data transmission mechanisms necessary for the parties to perform their obligations under the Data Security Laws; (iii) complete any security questionnaires, IT rules of behavior, certifications, assessments, or workforce training reasonably requested by USAC in a timely manner; and (iv) receive prior written authorization from USAC to access USAC IT Systems from USAC. If at any time USAC determines that the establishment of such gateways or data transmission mechanisms is reasonably required to securely access the Services, their establishment shall be at Contractor's sole cost and expense. Under no circumstances shall USAC's written authorization to access USAC IT Systems serve as a representation or warranty by USAC that

such access is secure or as a waiver of any rights in this Privacy and Security Addendum or the USAC Standard Terms and Conditions. Failure to satisfy the conditions set forth in subsections (i) – (iv) herein to USAC's reasonable satisfaction shall be considered a material breach of the USAC Standard Terms and Conditions by Contractor.

2.4. Contractor Security Policies. Throughout the Contract Term, Contractor shall establish and maintain appropriate internal policies and procedures regarding: (i) the security of the Services and Contractor IT systems; and (ii) the permitted use, disclosure, access to, and security of PII, USAC Data, Confidential Information, and USAC IT Systems. Contractor shall provide USAC upon request with copies of its information privacy and IT security policies and procedures to review. Such policies and procedures shall not materially conflict with USAC's policies and procedures either expressly or by omission. Contractor agrees to maintain strict control of Contractor IT and the access information (e.g. name, username, password, access rights) of all Contract Staff, to immediately remove access for persons no longer authorized, and to inform USAC immediately if Contractor suspects, or reasonably should suspect, there is unauthorized access to USAC Data or the USAC IT System. Contractor shall require Contract Staff to use Multifactor Authentication. Contractor agrees to require all who have access to USAC IT Systems through Contractor to maintain the confidential nature of the Confidential Information, and to not use or access USAC IT Systems except for the benefit of USAC.

2.5. Compliance Plan. In providing the Services, Contractor's Data Safeguards shall be no less rigorous than the most protective of: (a) the requirements of applicable Law; (b) the specific standards set forth in this Article; and (c) the applicable USAC standards relating to data security. The parties shall execute an interconnection security agreement prior to any required establishment of direct interconnection between Contractor IT and USAC IT Systems.

2.6. PII. Contractor shall ensure that: (i) PII shall be protected in accordance with all laws and USAC requirements, including, without limitation, relevant: (a) OMB Memorandum M-17-12; (b) guidance from the NIST including without limitation the most current revision of NIST SP 800-53 Rev. 5; and (c) FCC requirements or the most current replacement of the above; (ii) to the extent that cloud-based Services are to be employed by Contractor and interact with USAC Data, Contractor shall provide documentation and proof of FedRAMP-Authorization to demonstrate compliance, and such Services shall be certified by FedRAMP for use at a moderate risk by the time the cloud-based Services are implemented (USAC reserves the right to inspect the Authority to Operate or the complete package of documents for those with agency accreditation); and (iii) all Cybersecurity Incidents or Privacy Incidents resulting in any interruption to system services, including the disclosure of PII, shall be tracked in accordance with NIST SP 800-53 Rev. 5, NIST SP 800-61, and OMB Memorandum M-17-12.

2.7. Contractor Responsible for Contract Staff. Contractor shall ensure that all Contract Staff will be bound by the same or substantially similar restrictions on collection, use, disclosure, and retention of PII, Confidential Information, USAC Data, and USAC Software. Contractor shall be responsible for any breach of data security or privacy-related obligations by any Contract Staff and shall fully indemnify USAC for any damages incurred as a result of such breach.

Universal Service Administrative Co.

Contractor will be required to provide annual information security and privacy awareness training to all Contract Staff that will be working under the USAC Standard Terms and Conditions prior to having access to USAC Data or to USAC IT Systems. All Contract Staff will also be required to sign USAC's IT rules of behavior as well as confidentiality and non-disclosure agreements as required by third parties and USAC.

2.8. Vendor Insider Threat Program. Vendor will submit Vendor's insider threat program (as required by NIST 800-53 Rev. 5 (see controls PM-12, IR-4(6), IR-4(7), and SI-4(12)) to USAC's Chief Privacy Officer and USAC's Chief Information Security Officer within ninety (90) days of the Effective Date of the Contract. If USAC has any questions regarding Vendor's insider threat program, Vendor will make Contract Staff knowledgeable of Vendor's insider threat program available to USAC upon USAC's request.

2.9. Encryption and Secure Storage. PII must be encrypted at all times in accordance with FIPS 140-3 standards. This encryption requirement includes both Data at Rest and Data in Transit. Any PII that is retained in documents or other physical formats must be stored in a secured location and with limited access. The standard for disposal of PII requires practices that are adequate to protect against unauthorized access or use of the PII, including at minimum adhering to the provisions of the USAC Terms and Conditions and this Privacy and Security Addendum.

2.10. Further Requirements. Contractor's applications, processes, and systems used in providing the Services shall be approved by USAC's IT security team and shall comply with FISMA, NIST, and OMB requirements. Contractor shall demonstrate Authority to Operate for any system that will temporarily or permanently house USAC Data, in compliance with NIST standards, and will provide all relevant documentation as defined in the NIST RMF lifecycle therein. Contractor further agrees to provide any assistance requested by USAC to enable Contractor or USAC to comply with FISMA requirements, including, without limitation, at Contractor's expense, providing USAC with periodic documentation and reports demonstrating FISMA compliance, system accreditation, and correction of any weakness or deficiency (as defined by FISMA) attributable to Contractor that would prevent Contractor or USAC from complying with FISMA. Contractor shall be responsible at its sole expense to remediate any FISMA noncompliance of its systems or the Services. No less than annually, Contractor shall write, review, and update an assessment of its compliance with all applicable federal mandates and other industry-accepted standards as set forth in this Article to ensure adherence thereto. Contractor will also perform any and all activities needed to ensure continued compliance with all federal mandates and other industry-accepted standards as set forth in this Article. *[This provision is applicable to contracts for procuring new information technology systems/tools only].*

2.11. Contractor Assumption of the Risk. Contractor agrees that access to PII, USAC Data, Confidential Information, and USAC IT Systems is at USAC's sole discretion, and that Contractor's access to such systems or information may be conditioned, revoked or denied by USAC at any time, for any reason, without any liability whatsoever to USAC. Access to USAC IT Systems by Contractor and Contract Staff, including any data-sharing or interoperability

Universal Service Administrative Co.

between USAC and Contractor, shall be for the sole purpose of providing the Services. Contractor agrees that: (i) USAC IT Systems are owned solely by USAC; (ii) USAC will monitor the use of USAC IT Systems; (iii) neither Contractor nor Contract Staff have any expectation of privacy with regard to USAC IT Systems; and (iv) all information appearing on USAC IT Systems (except for information publicly disclosed by USAC) will be considered Confidential Information. Contractor will not use USAC IT Systems except as expressly authorized by USAC. USAC requires that Contract Staff use a USAC.org email address when providing Services. Contractor agrees that its use of, and access to, USAC IT Systems is completely at its own risk.

2.12. Contractor's Obligation for Subcontractors. Contractor agrees to ensure that any subcontractor that accesses, receives, maintains, or transmits PII, USAC Data, Confidential Information, or USAC IT Systems agrees to the same restrictions and conditions that apply to Contractor under this Privacy and Security Addendum and the USAC Standard Terms and Conditions.

2.13. Performance Within United States. All Services must be performed within the United States. This requirement is inclusive of: (a) work related to the Services performed by all Contract Staff; and (b) storage and/or processing of data and/or other virtual Services (such as cloud storage, remote data processing, *etc*.).

2.14. Cybersecurity Incidents and Privacy Incidents

2.14.1. Contractor Must Notify USAC of Cybersecurity Incidents and Privacy Incidents. Contractor shall examine any Event that is an exception to the normal operation of IT infrastructure, systems, services, or privacy in order to identify if the Event represents a threat, an attack, or a breach. Any Event identified as a Cybersecurity Incident or Privacy Incident requires that USAC be notified at incident@USAC.org and Privacy@USAC.org within one (1) hour of becoming aware of an actual or suspected Cybersecurity Incident or Privacy Incident.

2.14.2. Notification Requirements. Contractor's notice to USAC shall include the following: (i) a description of the Cybersecurity Incident or Privacy Incident, including the date of the Cybersecurity Incident or Privacy Incident and the date of discovery by Contractor, if known; (ii) a description of the type(s) of Malicious Code, PII, USAC Data, Confidential Information, or USAC IT Systems involved in the Cybersecurity Incident or Privacy Incident, if any; (iii) if applicable and to the extent possible, a list of each individual whose PII has been, or is reasonably believed to have been accessed, acquired, used, or disclosed during or as a result of the Cybersecurity Incident or Privacy Incident; (iv) a brief description of what Contractor is doing to investigate the Cybersecurity Incident or Privacy Incident and mitigate the harm to USAC; (v) any steps Contractor recommends USAC should take to protect itself from potential harm resulting from the Cybersecurity Incident or Privacy Incident; (vi) the name, phone number, and e-mail address of Contractor's representative responsible for responding to the Cybersecurity Incident or Privacy Incident; and (vii) any information required

for USAC to comply with the Data Security Laws. Upon receiving Contractor's initial notice, USAC shall have the right to immediately take any security measures it deems reasonably necessary to mitigate the harmful effects to the PII, USAC Data, Confidential Information, or the USAC IT Systems. Contractor will regularly supplement its notice(s) with additional information as it becomes available.

2.14.3. Contractor Responsibilities Prior-to and After Cybersecurity Incident or Privacy Incident. Contractor, working with USAC, shall use its best efforts to mitigate and eliminate the effects of the Cybersecurity Incident or Privacy Incident on USAC and, if the Cybersecurity Incident or Privacy Incident causes any loss of operational efficiency, loss of data, or unauthorized disclosure, Contractor will assist USAC in mitigating or restoring such losses or disclosures. Contractor agrees to fully cooperate with USAC in the investigation of the Cybersecurity Incident or Privacy Incident (including participating in any needed forensic investigation and law enforcement investigations) and to participate in, to the extent directed by USAC, the notification of individuals, the media, the FCC, or third parties. Contractor shall promptly respond to USAC's questions regarding the Cybersecurity Incident or Privacy Incident and coordinate with Contract Staff if required to mitigate the harm. To the extent USAC determines necessary, USAC agrees to provide reasonable access to the affected systems in order for Contractor to assist in such restoration of efficiency or data. Notwithstanding anything to the contrary in the USAC Standard Terms and Conditions, if the Cybersecurity Incident or Privacy Incident is due to the negligence or misconduct of Contractor or Contract Staff, then Contractor shall: (i) perform its obligations under this Section at no cost to USAC; (ii) promptly implement or develop any additional protocols, policies, gateways, transmission mechanisms, or security layers, if reasonably necessary, at its sole cost and expense, and with the approval of USAC; (iii) indemnify USAC for all damages, and if needed PII breach mitigations, under this Section as a result of the Cybersecurity Incident or Privacy Incident. Failure to strictly abide by the USAC Standard Terms and Conditions and this Privacy and Security Addendum shall be considered a material breach of the USAC Standard Terms and Conditions for which USAC shall have the right to immediately terminate for cause.

2.15. Backups. Contractor shall automatically make backups of all USAC Data files found in Contractor's information technology systems. Such backup shall be in a format that is readily accessible and usable by USAC.

2.16. Security Audit. USAC or its designated USAC auditor may, at USAC's expense and at any time, perform an audit of the security policies and procedures implemented by Contractor and in effect at Contractor locations. Contractor is responsible for remediation of any identified weakness or findings of noncompliance.

2.17. Security and Privacy Assessments. Contractor shall provide support for assessments of FISMA compliance on an annual basis. Security and privacy assessments may include, but are not

limited to, third party assessments to achieve FISMA ATO or to maintain continuous monitoring and ongoing authorization of a Contractor IT system in compliance with the RMF and controls described in NIST SP 800-53 Rev 5. The assessment process may also include security penetration testing to identify additional vulnerabilities through ethical hacking and compliance challenging techniques. Assessments shall include but shall not be limited to: (a) Contractor's documented and demonstrated internal controls and procedures related to the Services; (b) cooperation with USAC IT security or privacy staff in connection with testing the effectiveness of such controls and procedures; (c) making at least quarterly representations to USAC regarding any significant changes to such controls and procedures; (d) documenting and tracking all identified material weaknesses or deficiencies reported by an assessment, penetration test, Cybersecurity Incident, Privacy Incident, or any other deficiency that would prevent USAC from complying with law, using a Plan of Action and Milestones ("POA&M") process; and (e) cooperating with USAC auditors in connection with the issuance of the reports described in Section 2.20 of this Privacy and Security Addendum. Contractor shall promptly remediate any weakness identified in any assessment, in no event later than recommended or demanded by the assessors. *[This provision is applicable to contracts for procuring new information technology systems/tools only].*

2.18. Notification and Assistance. Contractor will cooperate with USAC in any litigation and investigation deemed necessary by USAC to protect USAC Data, other USAC Confidential Information, and/or PII. Each party will bear the costs it incurs as a result of compliance with this Section.

2.19. Vulnerability Management. Contractor shall address vulnerabilities in accordance with NIST vulnerability management controls including, but not limited to, addressing vulnerabilities in the applicable timeframes set forth in such policies. Contractor shall provide a monthly vulnerability report and a risk mitigation plan to address any identified vulnerabilities. Critical and high vulnerabilities, as defined in NIST management controls, shall be reported to the USAC Chief Information Officer and Chief Information Security Officer, and Contractor shall remedy such vulnerabilities as soon as possible. Contractor shall provide USAC a POA&M to address such vulnerabilities promptly and shall prioritize remediation based on the risks implicated by such vulnerabilities.

2.20. Additional Requirements for Services in Contractor IT

- If Contractor becomes aware that the Services in Contractor IT will lose or has lost its respective FedRAMP Authorization, Contractor shall notify USAC within twenty-four (24) hours, shall discontinue use of such Services, and shall initiate activities to replace the Services that have lost FedRAMP Authorization. Contractor and USAC shall work together to identify a replacement solution. A replacement solution must be identified and approved in writing by USAC within ten (10) business days of the initial FedRAMP Authorization changes notification.

- Contractor shall implement and use Cloud Protocols in connection with the Services operated in cloud infrastructure environments provided and controlled by any third-party. USAC's receipt of the Services and Contractor's and USAC's use of the Services shall be in accordance with such Cloud Protocols.

- Contractor shall maintain Contractor IT used by Contractor in performance of the Services. USAC may require Contractor to respond to the information security questionnaires regarding Contractor's information security policies and practices. USAC will conduct its information security review, if required, with reference to the responses Contractor provides to such information security questionnaires. At USAC's request, Contractor shall also respond promptly (within 10 business days) to any new or supplemental information security questions that USAC may require of Contractor during performance. USAC may terminate the Contract upon notice if Contractor fails to provide a timely response to requests for new or supplemental information security information or if USAC determines that Contractor's information security policies or practices increase risk to USAC in a manner unacceptable to USAC.

- Contractor shall maintain administrative, technical, physical, and procedural information security controls compliant with ISO 27001 standards for all Contractor IT used by Contractor in performance of the Services. Contractor shall maintain ISO 27001 compliance certification and notify USAC of any changes to its compliance. Contractor shall provide USAC with its ISO 27001 compliance certification within ten (10) calendar days of the Effective Date.

- Contractor shall maintain administrative, technical, physical, and procedural information security controls as demonstrated in Service Organization Controls ("SOC") 2 Type II reports. Contractor shall maintain these controls and notify USAC of any changes to its compliance. Contractor shall provide USAC with its most current SOC 2 Type II report within ten (10) calendar days of the Effective Date.

- On an annual basis, upon written request, Contractor will provide USAC with the most current versions of following:

    - Contractor security policies referenced in Section 2.4 of this Privacy and Security Addendum;
    - Standard Information Gathering (SIG) Lite documentation;
    - SOC 2 Type II report;
    - System ATO(s) or evidence of effective Information Security Continuous Monitoring (ISCM) in compliance with FISMA and NIST SP 800-53 Rev. 5;
    - ISO 27001 certifications.

[This provision is applicable to contracts for procuring new information technology systems/tools only]

3. TECHNOLOGY CONSIDERATIONS

Universal Service Administrative Co.

3.1. Deployment in Cloud. Contractor shall ensure that SaaS, PaaS, or IaaS Cloud Service Offerings, or COTS, deployed in Contractor IT cloud or on any USAC-acquired CSP infrastructure, satisfies the following requirements:

3.1.1. The Software must be able to utilize USAC's instance of OKTA's identity and access management software for user authentication and provisioning. OKTA is a FedRAMP Authorized CSP identity and access management product used by USAC.

3.1.2. Any USAC Data stored in a database that is a component of a CSP SaaS, PaaS, or IaaS, or a COTS, must be readily available to USAC in industry standard formats that enable USAC to access, copy, or transfer USAC Data as required.

3.1.3. Any SaaS, PaaS, or IaaS Software must maintain the Authority to Operate and FedRAMP Authorization for the Contract Term.

3.2. Custom Software. Contractor shall ensure that any custom Software developed and/or deployed for USAC, whether on USAC premise, on a USAC or Contractor cloud, or on a hybrid infrastructure:

3.2.1. Meets all USAC architecture, standards, and IT security guidelines and standards. This includes, but is not limited to, the ability to achieve an Authority to Operate based on all applicable OMB, NIST, and FISMA guidelines.

3.2.2. Reuses available USAC technology services (including microservices and application programming interfaces) unless Contractor demonstrates in writing that those services are unable to meet the requirements and USAC agrees to the substitute solution in writing with Contractor.

3.2.3. Uses the USAC technical stack unless Contractor demonstrates in writing that those components are unable to meet the requirements and USAC agrees in writing with Contractor. Details of USAC's technical stack and service architecture will be provided as appropriate.

3.3. Artificial Intelligence. Any actual or proposed use of AI by Contractor, including but not limited to use in solutions, processing, document reviews/analysis, or management of USAC systems or processes ("AI Use"), shall be governed by the AI Authorization Addendum, which is hereby incorporated into the Contract.

4. MALICIOUS CODE AND MALICIOUS CYBER ACTIVITIES

USAC may provide Contractor access to one or more USAC IT Systems. Contractor agrees that the USAC IT Systems are owned by USAC, that USAC reserves the right to monitor use of the USAC IT Systems, that neither Contractor nor Contract Staff should have any expectation of privacy with regard

to use of USAC IT Systems, and that all information appearing on USAC IT Systems (except for authorized information provided by Contractor or information publicly disclosed by USAC) will be considered as USAC Confidential Information. Contractor agrees that it will not use USAC IT Systems except as expressly authorized by USAC in this Privacy Security Addendum and the USAC Standard Terms and Conditions. Contractor agrees to maintain strict control of all Contract Staff usernames, passwords, and access lists for USAC IT Systems, to immediately remove such access for those persons no longer authorized, and to inform USAC immediately if there is reason to believe there is unauthorized access Contractor agrees to cause all who gain access to USAC IT Systems through Contractor to maintain the confidential nature of all Confidential Information, and to not use USAC IT Systems except for the benefit of USAC. Contractor agrees that it will use USAC IT Systems completely at its own risk, and that it will be liable to USAC for any damages incurred by USAC as a result of Contractor's violation of this Section.

Contractor will not introduce Malicious Code into USAC IT Systems or engage in Malicious Cyber Activities in, with, or involving the Services or USAC IT Systems. For any aspect of the Services in Contractor IT, Contractor will comply with NIST SP 800-83 Rev. 1 or the most current revision thereof to prevent Malicious Code. Contractor will perform regularly scheduled (preferably in real-time, but in no event less frequently than daily) virus checks using the latest commercially available, most comprehensive virus detection and scanning programs. If Contractor becomes aware that Contractor introduced Malicious Code into any USAC IT System, or engaged in Malicious Cyber Activities, Contractor will notify USAC immediately. In addition, Contractor will use its best efforts to assist USAC in reducing the effects of the Malicious Code or Malicious Cyber Activities. If the Malicious Code or Malicious Cyber Activity causes a loss of operational efficiency or loss of data, Contractor will assist USAC in mitigating and restoring such losses. USAC will provide reasonable access to the affected systems in order for Contractor to assist in such restoration of efficiency or data. If Malicious Code is found to have been introduced into any USAC IT System or the Services, Contractor will perform all of its obligations under this Section at no cost to USAC, and Contractor will be liable to USAC for damages and costs incurred by USAC as a result of such Malicious Code. If Contractor or Contract Staff has been found to (a) have engaged in any Malicious Cyber Activities; or (b) have allowed Malicious Cyber Activities to have occurred due to its willful, reckless, or negligent actions or omissions, Contractor will be liable to USAC for damages and costs incurred by USAC as a result of such Malicious Cyber Activities.

If Malicious Code is introduced into USAC IT Systems, and/or Contractor or Contract Staff has engaged in Malicious Cyber Activity involving USAC IT Systems, it shall be considered a Cybersecurity Incident or Privacy Incident. If Contractor becomes aware that Malicious Code has been introduced into USAC IT Systems, or Contractor or Contract Staff has engaged in Malicious Cyber Activity, Contractor will notify USAC within one (1) hour of becoming aware.

Universal Service Administrative Co.

USAC STANDARD TERMS AND CONDITIONS

ARTIFICIAL INTELLIGENCE AUTHORIZATION ADDENDUM

This Artificial Intelligence Authorization Addendum ("AI Authorization Addendum") is entered into as of [INSERT DATE] by and between Universal Service Administrative Company ("USAC") and [ ] ("Contractor").

This AI Authorization Addendum supplements and is incorporated into the USAC Standard Terms and Conditions, dated [DATE], between USAC and Contractor, the Privacy and Security Addendum, and all applicable statements of work (collectively, the "Contract"). Capitalized terms used but not defined herein shall have the meanings ascribed to such terms in the Contract.

An "AI Model" is a capability used to process information and inputs in order to produce outputs such as predictions, classifications, embeddings, or generated content. An "AI System" is a system that uses one or more AI techniques or AI Models to interpret inputs and produce an output that supports or performs a task, such as a prediction, recommendation, classification, generated response, decision, or action, depending on what the system is designed to do.

For purposes of this AI Authorization Addendum, "USAC Data" includes all data made available by or on behalf of USAC or accessed in performing the Contract, including, but not limited to, Confidential Information, PII, inputs, prompts, queries, documents, records, source code, output, logs, metadata, usage data, feedback, embeddings, vectors, model weights, fine-tuning materials, and derivatives.

The Contract prohibits Contractor's AI Use except where USAC provides prior written approval. This AI Authorization Addendum constitutes USAC's limited written approval solely for the AI system(s), use case(s), USAC Data category or categories, and time period expressly identified below in an attached Exhibit A - Approved AI Use Schedule. All AI Use pursuant to the Contract is governed by this AI Authorization Addendum and all proposed AI Use must be expressly identified in Exhibit A and approved by USAC in writing. USAC's written approval for any AI Use will be communicated to Contractor by USAC's Contract Administrator for the Contract.

1. AUTHORIZED AI USE

Subject to Contractor's continuous compliance with the Contract and this AI Authorization Addendum, USAC authorizes Contractor to use only the AI System(s) identified in the Approved AI Use Schedule attached as Exhibit A (each, an "Approved AI System").

Contractor may use each Approved AI System solely:

a. For the specific purposes and workflows identified in Exhibit A;
b. During the authorized period stated in Exhibit A;
c. Using only the personnel, subcontractors, and categories of USAC Data expressly identified in Exhibit A; and

Universal Service Administrative Co.

d. In accordance with all data, security, human-review, testing, monitoring, output-control, and all other conditions, restrictions, and guidelines stated in the Contract, this AI Authorization Addendum, and Exhibit A.

Use, uploading, input, processing, or otherwise making available USAC Data, Confidential Information, and/or PII in any AI tool (including third-party or public models) must be expressly disclosed in an Approved AI Use Schedule, requires prior written authorization from USAC, and must comply with all applicable privacy laws and USAC security requirements as specified in the Contract.

Nothing in this AI Authorization Addendum is intended to provide any authorization not explicitly granted through this section, including, but not limited to, the authorization for Contractor to use another AI System, another AI Model or version, a different provider, a different hosting environment, a different data category, or a different use case without USAC's prior written approval. Additionally, Contractor shall not make any material change to an Approved AI System – including, but not limited to, a change to its provider, model, model version, architecture, hosting environment, geographic processing location, integrated tools, connectors, data-retention setting, training setting, or permitted data – without USAC's prior written approval. Approval for any changes identified in this paragraph must be obtained through the submission and approval of a revised or additional Approved AI Use Schedule identifying the material change to the Approved AI System.

In conjunction with seeking written approval pursuant to this Addendum, Contractor shall disclose all third-party AI Use, including models, underlying engines, and sub-processors utilized, leveraged, or incorporated into its proposed AI System or AI tools it intends to use in its performance under this Contract. Disclosure shall include the third-party AI Model's training data sources (including large language models), training methodology, learning cutoff dates, and model limitations. Contractor shall provide USAC with advanced written notice, including the submission and approval of a revised Approved AI Use Schedule, if it intends to switch or use new third-party AI tools and models during the course of this Contract. Contractor shall be solely responsible for ensuring, on an ongoing basis, that third-party AI operates in accordance with the Contract and this AI Authorization Addendum. All Contractor obligations, standards of care, warranties and indemnifications apply equally to third-party AI. Contractor must ensure AI Use by its subcontractors and third parties complies with this AI Authorization Addendum. Contractor remains responsible for their subcontractors' AI-related activities.

USAC may suspend or revoke authorization for an Approved AI System immediately upon written notice to Contractor if USAC reasonably determines, at its sole discretion, that continued use creates an unacceptable privacy, security, legal, intellectual property, operational, financial, or reputational risk. Contractor shall immediately stop the affected use upon receipt of such notice.

2. USAC AI MODELS

"USAC AI Model" means any AI Model, fine-tuned model, model weight, embedding, retrieval-augmented-generation system, vector database, prompt library, evaluation dataset, training dataset, model documentation, configuration, output, or other AI-related asset that is: (a) owned, licensed, developed, commissioned, funded, or made available by or for USAC by an entity other than Contractor; (b) trained,

Universal Service Administrative Co.

fine-tuned, configured, or materially improved using USAC Data at USAC's direction; or (c) designated by USAC in writing as a USAC AI Model.

As between the parties, USAC owns all rights, title, and interest in and to USAC AI Models and all USAC Data used in connection with them.

Contractor receives only a limited, non-exclusive, non-transferable, non-sublicensable, revocable right to access and use an USAC AI Model solely as necessary to perform the specifically authorized Services for USAC.

Contractor shall not:

- Copy, download, extract, reverse engineer, decompile, disassemble, benchmark, test, analyze, or attempt to derive the source code, model weights, architecture, prompts, training data, or internal operation of any USAC AI Model;
- Use a USAC AI Model, its outputs, prompts, evaluations, embeddings, configurations, or derivative materials to benefit Contractor, an affiliate, another customer, or any third party;
- Use USAC AI Model assets to train, fine-tune, improve, evaluate, benchmark, or support another AI system;
- Disclose USAC AI Model assets or access credentials to any unapproved person; or
- Assert any ownership, lien, security interest, or other right in or to a USAC AI Model.

Upon expiration, termination, or USAC's request, Contractor shall immediately stop using USAC AI Models and return or securely delete all USAC AI Model materials in its possession or control, subject only to any legally required retention.

3. DATA USE; NO TRAINING; NO PROVIDER IMPROVEMENT

Except as expressly stated in Exhibit A, Contractor shall not use, and shall ensure that no AI provider, subcontractor, affiliate, or other third-party uses, USAC Data for AI Model or tool training (including, but not limited to, pre-training, fine-tuning, evaluation, validation, testing, maintenance, model improvements, analytics, benchmarking, research, advertising, new AI Model development or creation), or any purpose other than the provision of the Services.

Contractor shall configure each Approved AI System, to the extent commercially and technically feasible, to: (a) disable use of USAC Data for Contractor or third-party training and model improvements; (b) minimize retention of USAC Data; (c) prohibit public sharing and external disclosure; (d) limit access through least-privilege controls (*e.g.*, granting minimum access and permissions to perform specific functions) and multi-factor authentication; and (e) segregate USAC Data from Contractor's and other customers' data. Any USAC Data that is incorporated into the AI System's functionality (*i.e.* AI System learning via USAC Data) as a product of Contractor's work for USAC must be removed from the AI System at the conclusion of the Contract Term.

Universal Service Administrative Co.

If Exhibit A expressly authorizes training, testing or fine-tuning using USAC Data, such work must occur solely in a logically segregated environment dedicated to USAC. Contractor shall not use any resulting model, model weight, embedding, evaluation result, or derivative for any person or entity other than USAC.

4. OUTPUT, HUMAN REVIEW, AND DECISION CONTROLS

All Deliverables (whether draft or final), outputs from Approved AI Systems used in the performance of this Contract (including, but not limited to, text, images, code, designs, classifications, labels, patterns, insights, data and reports), and Derivative Works from Deliverables and/or outputs are the sole and exclusive property of USAC. Contractor shall have no ownership rights or any proprietary interests whatsoever in the Deliverables, outputs or Derivative Works produced by or resulting from Contractor's use of Approved AI Systems in the performance of this Contract. To the extent necessary to ensure USAC ownership, Contractor hereby assigns to USAC all rights, title and interest in the aforementioned Deliverables, outputs and Derivative Works.

Contractor shall ensure that personnel with appropriate and applicable expertise review and validate the Approved AI System's AI-generated output (including, but not limited to, text, images, code, designs, classifications, labels, patterns, insights, data and reports) before using it to perform the Services, incorporating it into a Deliverable, communicating it to USAC or a third party, or relying on it for any decisions or recommendations. Contractor shall incorporate human review and oversight of an Approved AI Systems' on-going work under the scope of this Contract to ensure the protection of USAC Data and the accuracy and validity of AI-generated output.

Contractor remains fully responsible for all Services, Deliverables, recommendations, decisions, and work product, regardless of whether an AI System assisted in producing them. Use of an Approved AI System does not reduce, revise, amend, or otherwise affect Contractor's obligations, warranties, standard of care, or liability under the Contract. Any Approved AI System may support, but never replace or override, USAC staff or Contractor Staff responsible for decision-making of any kind, especially for areas that affect program beneficiaries or operations.

Contractor shall not use an Approved AI System or AI generated output as the sole or determinative basis for a decision with legal, employment, financial, benefits, insurance, education, healthcare, safety, eligibility, case outcomes, surveillance, or other material effect unless USAC expressly authorizes that use in Exhibit A, and Contractor implements meaningful human review per the above and fully documented validation procedures.

5. WARRANTY REGARDING REGULATORY COMPLIANCE

Contractor warrants that its use of Approved AI Systems complies with all applicable laws, regulations and industry standards including, but not limited to, United States federal and applicable state AI statutes and regulations. If changes in law require a modification to an Approved AI System, Contractor shall make the necessary modifications at no additional cost to USAC and within thirty (30) days of such law going into effect. If such modification constitutes a material change, Contractor must submit, and USAC must approve in writing, a revised Approved AI Use Schedule identifying the material change to the Approved AI System.

Universal Service Administrative Co.

Contractor shall comply with USAC's Secure and Trustworthy Artificial Intelligence Policy, plus all related USAC privacy/security policies, including the Privacy and Security Addendum, and applicable laws. This AI Authorization Addendum controls over conflicting Contractor policies.

6. VERIFICATION AND AUDIT

Contractor shall monitor each Approved AI System for material accuracy, reliability, bias, discrimination, security, confidentiality, potential intellectual property infringement, and legal-compliance risks before and during its use. Contractor shall promptly suspend use and notify USAC if it identifies a material risk, malfunction, or nonconformity.

USAC may, upon ten (10) days' notice, audit Contractor's Approved AI System to assure compliance with the Contract and this AI Authorization Addendum. USAC agrees to use reasonable efforts to avoid material disruption to Contractor's provision of the Services. Contractor agrees to provide USAC with access to documentation, logs, personnel and any other materials reasonably necessary to perform the audit. Contractor is responsible for remediation of any identified noncompliance.

7. AI INCIDENT RESPONSE

Contractor shall provide written notice to USAC within one (1) hour at incident@USAC.org and Privacy@USAC.org after any actual or reasonably suspected AI Incident and comply with all other notification requirements outlined in Section 2.14 of this Contract's Privacy and Security Addendum. "AI Incident" includes, but is not limited to, unauthorized AI Use; AI Use in excess of the scope of written approval; unauthorized access to, disclosure of, loss of, alteration of, or inability to access USAC Data through an AI System; prohibited retention of training data; any external attack (including, but not limited to, prompt injection and data exfiltration); harmful or materially inaccurate output; hallucinations; potential intellectual property infringement; model compromise; security vulnerability; an AI System's access to or use of unauthorized USAC systems, databases, or repositories; any Cybersecurity or Privacy Incident (as defined in Section 2.14 of this Contract's Privacy and Security Addendum) involving or caused by an AI System; or any breach of the Contract or this AI Authorization Addendum.

Contractor shall immediately, at its own cost: (a) investigate, contain, mitigate, and remediate the AI Incident; (b) stop the affected AI Use if directed by USAC or if reasonably necessary to prevent further harm; (c) preserve relevant logs, records, prompts, inputs, outputs, configurations, and evidence; (d) provide USAC with written status updates at least every four (4) hours until containment of the AI Incident and then daily until full remediation; (e) provide USAC with a full written report of the cause of the incident and precautions that will be put in place to help prevent further AI Incidents; and (f) cooperate fully with USAC's investigation, legal obligations, regulatory communications, and remediation efforts.

Contractor shall not notify any individual, customer, regulator, insurer, media outlet, AI provider, or any other third party of an AI Incident involving USAC Data without USAC's prior written approval, unless legally required. If legally required, Contractor shall provide USAC with adequate and reasonable advance

written notice to the extent permitted by law and cooperate with USAC regarding the content and distribution of the notice.

8. AI USE INDEMNIFICATION

Contractor shall indemnify, hold harmless, and defend USAC and its directors, officers, employees, and agents against any and all demands, claims and liability, costs and expenses (including attorney's fees and court costs) arising from or related to Contractor's use of AI or third-party AI tools in performance of this Contract, which are directly or indirectly related to: (a) any claims or demands for actual or alleged direct or contributory infringement of, or inducement to infringe, or misappropriation of, any intellectual property, including, but not limited to, trade secrets, patents, trademarks, service marks, or copyrights; (b) any claims, demands, regulatory violations, or government investigations related to a Cybersecurity or Privacy Incident; (c) any claims or demands related to discrimination, retaliation, or unlawful employment and hiring practices under state or federal law; and (d) any claims or demands related to or arising out of AI hallucinations or other materially inaccurate AI outputs (including, but not limited to, text, images, code, designs, classifications, labels, patterns, insights, data and reports).

Universal Service Administrative Co.

ARTIFICIAL INTELLIGENCE AUTHORIZATION ADDENDUM

EXHIBIT A: APPROVED AI USE SCHEDULE

1. Contractor: [Full Legal Name]

2. Related Contract/SOW: [Contract date and SOW number]

3. Authorization Effective Date: [Date]

4. Authorization Expiration Date: [Date]

5. Approved AI System(s)
   - Provider: [Name]
   - Product/service: [Name]
   - Deployment: [Ultimate-hosted/private tenant/contractor-hosted/provider hosted]
   - Processing and storage locations: [Locations]
   - Approved integration, connectors, APIs, or plug-ins: [List or "None"]
   - Approved subcontractors and AI providers: [List or "None"]

6. Authorized use case
   - Specific purpose: [For example: "Drafting internal summaries of non-confidential operation reports"]
   - Permitted workflow: [Describe]
   - Authorized users: [Name, roles, or limited user group]
   - Prohibited uses specific to this system: [Describe]

7. Authorized USAC Data
   - Permitted data categories: [List]
   - Prohibited data categories: [List –e.g. PII, source code, security data]
   - Data minimization/redaction requirements: [Describe]

8. Training, retention, and data controls
   - Provider training/model improvements on USAC Data: Prohibited/Authorized only as follows: [described]
   - Contractor training/fine-tuning using USAC Data: Prohibited/Authorized only as follows: [Describe]
   - Input/output retention period: [Period]
   - Logging requirements: [Describe]
   - Deletion requirements: [Describe]
   - Required settings: [No training enabled; no public sharing/no external browsing; encryption etc.]

Universal Service Administrative Co.

9. Human Oversight and Testing
   - Required reviewer: [Role/name]
   - Decisions the system may not make: [List]
   - Required Testing, validation, and monitoring: [Describe]
   - Output labeling/disclosure requirement: [Describe]

10. Additional Conditions

[Insert any specific, security, compliance, audit, insurance, or other requirements]

SECTION D:

ATTACHMENTS

- Attachment 1: Bid Sheet (Attached Separately)
- Attachment 2: USAC Confidentiality Agreement (Attached Separately)
- Attachment 3: Design Responsibility and Accountability Term (Attached Separately)
- Attachment 4: Key Personnel Resumes (Offerors shall submit resumes as Attachment 4)

Universal Service Administrative Co.

SECTION E:

INSTRUCTIONS AND EVALUATION CRITERIA

1. GENERAL

A. CONTRACT TERMS AND CONDITIONS

The Contract awarded as a result of this RFP will be governed by, and subject to, the requirements of all Sections of this RFP, including any attachments listed in Section D. Offeror's submission of a proposal constitutes Offeror's agreement to the RFP and its precedence over any other terms, requirements, or conditions proposed by Offeror. Offeror's submission must include a statement certifying that the USAC Standard Terms and Conditions set forth in this RFP have been reviewed by Offeror's office of general counsel (or equivalent legal representative).

Offeror's proposal may identify deviations from, or revisions, exceptions or additional terms (collectively "exceptions") to the RFP, but only if such exceptions are clearly identified in a separate Attachment to the proposal, "Exceptions to RFP Terms." Proposals that include material exceptions to the RFP may be considered unacceptable and render Offeror ineligible for award unless the Offeror withdraws or modifies any unacceptable exceptions prior to USAC's selection of the successful Offeror for award. USAC will only review and may consider changes or additions to the RFP that are included in Offeror's proposal. USAC reserves the right to eliminate a proposal from the evaluation process that includes material or unacceptable exceptions with or without notice to the offeror. After selection of the awardee, USAC will not consider or negotiate any exceptions to the RFP.

B. PERIOD FOR ACCEPTANCE OF OFFERS

Offeror agrees to hold the pricing in its offer firm for one hundred ~~twenty~~ eighty (~~120~~180) calendar days from the date specified for receipt of offers unless another time period is specified in an addendum to solicitation.

Proposals must:

- Precisely address USAC's requirements, as set forth in Section B. Statement of Work, and should not contain a significant amount of corporate boilerplate marketing information.
- Be submitted to USAC Procurement Department, no later than **11:00 AM ET on Monday, ~~November 23~~December 7, 2026** ("Proposal Due Date").
- Be submitted in the form of one electronic copy submitted to Procurement@usac.org with copy to Mustafa.Kamal@usac.org. The subject line for all email communication related to this solicitation must **only** be **RFP IT-26-148**.

Universal Service Administrative Co.

NOTE: Be advised that our mail server will automatically reject emails with lengthy subject-line.

C. PROPOSAL SCHEDULE

Key activities and target completion dates are set forth below. USAC may change these dates at its sole discretion and convenience, without liability.

DATE	EVENT
Monday, October 12, 2026	RFP Released
Tuesday , October 20, 2026	Questions due to USAC by 11:00 AM ET at Procurement@usac.org
~~Monday~~Friday, October ~~26~~30, 2026	Q&A responses released to potential offerors
Monday, ~~November 23~~December 7, ~~2025~~2026	Proposal Due to USAC by 11:00 AM ET at Procurement@usac.org copying Mustafa.Kamal@usac.org
TBD, 2026	Perform Proof of Concepts (If required)
TBD, 2026	Anticipated Award Date

To be timely, Offeror's proposal must be received by USAC by the Proposal Due Date at the email address specified above. Any offer, modification, revision, or withdrawal of an offer received at the USAC office designated in the solicitation after the Proposal Due Date and Time is late and will not be considered by USAC, unless USAC determines, in its sole discretion, that (1) circumstances beyond the control of Offeror prevented timely submission, (2) consideration of the offer is in the best interest of USAC, or (3) the offer is the only proposal received by USAC.

D. SUBMISSION OF QUESTIONS

USAC will only accept written (**MS Excel or MS Word**) questions regarding this RFP. All questions must be attached and emailed to Procurement@usac.org with a copy to Mustafa.Kamal@usac.org no later than **Tuesday, October 20, 2026, 11:00 AM ET**. USAC plans to post all questions and responses under this procurement on our website by **~~Monday~~Friday, ~~October 26~~December 7, 2026, by 5:00 PM ET.**

E. AMEND, REVISE OR CANCEL RFP

USAC reserves the right to amend, revise, or cancel this RFP at any time at the sole discretion of USAC. No legal or other obligations are assumed by USAC by virtue of the issuance of this RFP, including payment of any proposal costs or expenses, or any commitment to procure the services sought herein.

2. CONTRACT AWARD

Universal Service Administrative Co.

USAC intends to evaluate offers and make a single award. USAC may reject any or all offers if such action is in the public's or USAC's interest; accept other than the lowest offers; and waive informalities and minor irregularities in offers received. As stated in Section B.~~23~~20, USAC requires execution of Proof of Concepts with selected offerors during proposal evaluation, prior to contract award at no cost to USAC.

3. IDENTIFICATION OF CONFIDENTIAL INFORMATION

Offeror's proposal shall clearly and conspicuously identify information contained in the proposal that the Offeror contends is Confidential Information. See Section C.16.

4. PROPOSAL FORMAT

Proposals shall be presented in four separate volumes:

4.1. Volume 1 – Corporate Information
4.2. Volume 2 – Technical Capability
4.3. Volume 3 – Past Performance
4.4. Volume 4 – Price

5. PROPOSAL COVER PAGE

Each volume of Offeror's proposal must contain a cover page. On the cover page, please include:

- The name of Offeror's organization,
- Offeror's contact name,
- Offeror's contact information (address, telephone number, email address, website address),
- Offeror's Unique Entity ID number,
- The date of submittal,
- A statement verifying the proposal is valid for a period of one hundred ~~twenty~~ eighty (~~120~~180) days, and
- The signature of a duly authorized Offeror representative.

6. PRESENTATION AND PAGE LIMITATIONS

6.1. PROPOSAL PRESENTATION:

a. Proposals must be prepared using Times New Roman font. All text except for diagrams, tables, and charts must be presented in 12-point font. Diagrams, tables, and charts may be presented in a smaller font if needed to fit the page. The reduced font size may not be smaller than 9 points.

Universal Service Administrative Co.

b. The content of each diagram, table, Gantt chart, and chart must accurately depict the same information included in the text, serving as the visual representation of the written content in the proposal.

c. Any diagram, table, Gantt chart or chart must be readable when printed. These documents may be included as attachments to the proposal using landscape orientation to enhance presentation if needed.

d. All diagrams, tables, Gantt charts, and charts must be incorporated into the proposal using the native program from which it was created to eliminate distortion of text by inserting images and pictures.

e. The font color used to label column headings must be bolded and a contrasting color from the background color to clearly display headings.

f. Each volume of the proposal should be submitted in PDF format as a separate attachment to a single email to Procurement@usac.org with a copy to Mustafa.Kamal@usac.org. Attachment 1 – Bid Sheet may be submitted as a separate attachment in Excel format as an addition to Volume 4.

g. The signed Confidentiality Agreement may be submitted in PDF format as a separate attachment and will not count towards the page limits for volumes 1–4 of the Offeror's proposal.

6.2. PAGE LIMITATION

Page count for each volume, excluding the cover page, ~~and~~ table of contents, compliance matrix, Mandatory Requirements Certification, POC Test Plan, and Exceptions attachment, may not exceed the below:

Volume	Page Limit
Volume 1 – Corporate Information	Five (5) pages
Volume 2 – Technical Capability	Forty (40) pages, excluding Attachment ~~3~~4 (Resumes) and technical appendices
Volume 3 – Past Performance	Nine (9) pages
Volume 4 – Price	Six (6) pages

Note: Resumes must be submitted as a ~~separate~~ attachment 4 "Key Personnel Resumes" as required by Section E.7.B.15. Narrative summaries in lieu of formal resumes will not be accepted and will result in the proposal being evaluated as non-responsive.

7. PROPOSAL CONTENT

Universal Service Administrative Co.

The proposal shall be comprised of the following four (4) volumes:

A. Corporate Information (Volume 1)

1. **A cover page**, as outlined above.

2. **Executive Summary.** This section shall summarize all key features of the proposal, affiliated individuals, or firms that Offeror proposes to assist in this engagement. Pricing information shall not appear in the Executive Summary.

   ***NOTE**: If subcontractors are proposed, the Offeror must explicitly identify all proposed partners. Proposals featuring complex subcontracting structures (e.g., more than two subcontractors) must include a comprehensive coordination, management, and risk mitigation plan within this section.*

3. **Confidentiality and Information Security.** Offeror must explain in detail how they will establish and maintain safeguards to protect the confidentiality and integrity of USAC Confidential Information in their possession as required by the solicitation.

4. **Conflict of Interest.** Offeror must provide a statement regarding any known conflicts of interest. USAC is the appointed neutral administrator of the federal USF. USAC is governed by a Board of Directors comprised of various stakeholders in the universal service programs and is prohibited from advocating positions on universal service policy matters. Because of USAC's unique role as neutral administrator, it is essential that any contractor providing assistance to USAC in administering the USF maintain the same neutrality, both in fact and in appearance.

   a. USAC procurements are conducted with complete impartiality and with no preferential treatment. USAC procurements require the highest degree of public trust and an impeccable standard of conduct. Offerors must strictly avoid any conflict of interest or even the appearance of a conflict of interest, unless USAC has otherwise approved an acceptable mitigation plan.

   b. Offerors must identify any actual or potential conflicts of interest including current USAC vendors involving Offeror or any proposed subcontractor, or any circumstances that give rise to the appearance of a conflict of interest, and the means by which it proposes to avoid, neutralize, or mitigate such conflicts. Offerors shall identify such conflicts or potential conflicts or appearance issues to USAC and provide detailed information regarding the nature of the conflict. Examples of potential conflicts include, but are not limited to: (1) any ownership, control or other business or contractual relationship(s), including employment relationships, between Offeror (or proposed subcontractor) and any USF stakeholder; (2) Offeror has a direct personal or familial relationship with a USAC or FCC employee; (3) a former employee of USAC or FCC who had access to confidential procurement-related information works for Offeror; (4) an USAC or FCC employee receives any type of compensation from Offeror, or has an agreement to receive such compensation in the future; (5) Offeror has communications with a USAC or FCC employee regarding future employment following the issuance of the RFP for this

Universal Service Administrative Co.

procurement; (6) any employment or consultation arrangement involving USAC or FCC employees and Offeror or any proposed subcontractor; and (7) any ownership or control interest in Offeror or any proposed subcontractor that is held by an FCC or USAC employee. Offerors must also identify any participation by Offeror, or any proposed subcontractor(s) or personnel associated with Offeror, in any of the universal service programs. The requirement in this Section E.~~6~~7.A.4.b applies at all times until Contract execution.

c. Offerors shall propose specific and detailed measures to avoid, neutralize, or mitigate actual, potential and/or apparent conflicts of interest raised by the affiliations and services described above. If USAC determines that Offeror's proposed mitigation plan does not adequately avoid, neutralize or mitigate any actual or potential conflict of interest, or the appearance of a conflict of interest, Offeror will not be eligible for award of a contract.

5. **Platform Relationship Disclosure.** Disclosure of all resellers, referral, partner, marketing development fund, revenue share, rebate and equivalent commercial arrangements between the Offeror or any teaming partner and each platform the Offeror proposes or that is under evaluation, together with a proposed mitigation plan. USAC retains the right to make gate determinations on the basis of empirical POC data and its own analysis rather than Contractor recommendation. Failure to disclose such an arrangement is grounds for exclusion from award and/or for termination for cause.

6. **Company Profile and Scale.** To evaluate operational stability and mitigate risks associated with executing high-value, multi-year contracts, the Offeror must provide corporate metrics for its most recent completed fiscal year. This must include:

- Total annual revenue
- Total number of full-time employees
- *If the Offeror is a subsidiary or joint venture, provide these metrics for both the prime bidding entity and the parent organization.*

B. Technical Capability (Volume 2)

This volume must include a cover page and the following:

1. **Technical Approach:** An in-depth discussion of the Offeror's approach to providing the Services outlined in Section B, addressing each CLIN, and a clear statement of whether performance will comply with all requirements stated in this RFP, including the USAC Terms and Conditions in Section C. Any deviations or exceptions must be clearly identified in a separate Attachment.

2. **Proposed Platform and Authorization:** Identification of the specific platform proposed, its FedRAMP authorization status and authorization boundary, the hosting and tenancy model proposed, and confirmation that the core platform capability is delivered through a single authorized offering under a single authorization boundary.

Universal Service Administrative Co.

3. **Mandatory Requirements Certification:** A signed certification that the proposed platform satisfies every mandatory requirement in Section B.6.1, with a cross-reference to the evidence supporting each. Proposals that do not certify compliance with all mandatory requirements will not be evaluated further, subject to Section B.6.1.

4. **Platform Capability Compliance Matrix:** A matrix mapping each requirement in Section B.6 to the specific native platform feature, supported configuration, or integration that satisfies it, identifying which capabilities are native to the proposed offering and which require separate licensing. Statements that merely restate the requirement will be evaluated as non-responsive to that requirement.

5. **Proof of Concept Approach and Test Plan:** The Offeror's approach to executing the POC test cases in Section B.20.2, including instrumentation, methodology, and the evidence the Offeror will produce for each test case. Offeror shall develop and submit a POC Test Plan as part of its proposal submission. See Section B.20 for the POC requirements.

6. **Migration and Cutover Approach:** The Offeror's approach to data, pipeline, report and code migration; parallel operation; reconciliation; and phased cutover, including how the ~~mandatory floor~~minimum viable product in Section B.6.6 will be preserved.

7. **Business Intelligence Approach:** Treatment of Structure 1 and Structure 2 as described in Section B.6.6, including the Offeror's recommendation and the basis for it.

8. **Governance Approach:** Treatment of Option A and Option B as described in Section B.6.4, including the Offeror's recommendation and the basis for it.

9. **Geospatial Approach:** The Offeror's approach to geospatial ingestion, and processing,

10. **Usability:** A description of the human-computer interaction characteristics of the proposed platform for each principal USAC user population, identifying which tasks require engineering assistance under the proposed model, per Section B.6.6.

11. **Division of Work and USAC Staffing:** The proposed division of work between Contractor Staff and USAC personnel across every task area, and the number, role, skill set and level of effort of USAC personnel the Offeror assumes USAC will supply, per Section B.~~14.4~~11.4. Unstated assumptions about USAC-supplied effort will not be recognized as a basis for schedule relief or additional compensation.

12. **Ecosystem and Sustainability:** Evidence supporting the final mandatory requirement in Section B.6.1, including the size of the commercial user base for the proposed platform, the

availability of implementation and support resources from sources other than the Offeror, and the Offeror's assessment of USAC's ability to sustain the platform over a ten (10) year horizon.

13. **Security and Privacy Approach:** How the Offeror will satisfy Section B.8, including the handling of live production data in the final validation round.

14. **Capabilities:** The Offeror's capabilities for performing the Services, including personnel resources and management capabilities. If applicable, how subcontractors or partners are used, how rates are determined, and a list of firms to be used.

15. **Key Personnel:** Identification by name of all Key Personnel required by Section B.11, with a description of technical knowledge and experience related to the requested Services, and identification of any other personnel to be assigned and their roles. Resumes for all Key Personnel must be submitted as Attachment ~~3~~4, limited to a maximum of two (2) pages per resume.

    ***NOTE**:*

    A. The inclusion of formal, chronological resumes is mandatory. Narrative summary paragraphs provided in the body of the proposal in lieu of a formal resume is non-compliant and will result in the Key Personnel being deemed unqualified. If the Offeror has information that any Key Personnel anticipate terminating their employment or affiliation, the Offeror shall identify such personnel and the expected termination date.

    B. Technical proposals that merely repeat the requirements set forth in this RFP and state that the Offeror "will perform the statement of work" or similar verbiage will be considered technically unacceptable and will not receive further consideration. USAC is interested only in proposals that demonstrate the Offeror's expertise in performing engagements of this type as illustrated by the Offeror's description of how it proposes to perform the requirements set forth in this RFP.

16. **Use of Artificial Intelligence.** USAC will evaluate the Offeror's proposed use of AI in the performance of the Services in accordance with the Privacy and Security Addendum of USAC's Standard Terms and Conditions and Section B.6.7. The Offeror must provide an extensive, detailed narrative within their technical approach describing exactly how, where, and in what specific circumstances AI tools will be deployed to perform the Services, alongside a concrete business case outlining the direct, quantifiable benefit of this AI usage to USAC. This is distinct from, and additional to, the AI capability required of the platform itself under Section B.6.7. Offerors shall submit separate versions of Attachment 1 – Bid Sheet for scenarios with and without the use of AI in performance of the Services. Offeror will not be permitted to use, implement, build, or deploy AI tools, services, or code of any type in performance of this Contract without prior written approval from USAC.

C. Past Performance (Volume 3)

Universal Service Administrative Co.

This volume must include:

1. A cover page, as outlined above.

2. Description of the Offeror's recent experience providing services as detailed in Section B, with examples of projects and personnel, including types of positions and length of assignments.

3. A list of three (3) current or recently completed contracts for services similar in scope to those required by this solicitation. *To evaluate broad commercial capabilities, no more than one (1) of the three required contracts may be a prior or current contract with USAC. USAC is specifically looking for verified industry experience external to USAC.*

   a. For each past performance, provide a description of the relevant performance for each project discussed. A past performance description will consist of: (i) an overview of the engagement, (ii) a description of the scope of work performed, (iii) clear, objective documentation of its technical and operational relevance to this specific effort, and (iv) the results achieved. This is the time to identify any unique characteristics of the project, problems encountered, and corrective actions taken. Each overview shall not exceed one (1) page.

   b. USAC will attempt to contact past performance references identified in the proposal for confirmation of the information contained in the proposal by transmitting a past performance questionnaire via email to the point of contact(s) identified in Offeror's proposal. Although USAC will follow-up with the contacts, Offeror, not USAC, is responsible for ensuring that the questionnaire is completed and returned by the specified date in USAC's transmittal. If USAC is unable to reach or obtain a reference for the project, USAC may not consider the contract in an evaluation of past performance. Prior to submitting a reference in the proposal, Offeror should ensure a point of contact is available and able to provide a written response to USAC's request for a reference check via the past performance questionnaire.

   Each entry on the list **must** contain all of the following information without omission:

   - The client's name,
   - The project title,
   - The exact period of performance (explicit start and end dates/durations),
   - The contract number,
   - The total contract value,
   - A primary corporate point of contact (including a verifiable telephone number and official corporate or government email address; personal email domains such as gmail.com, yahoo.com, etc., are unacceptable), and
   - A back-up corporate point of contact with complete corporate contact information.

Universal Service Administrative Co.

***NOTE**: Failure to provide full contract values, explicit durations, valid phone numbers, or corporate email addresses may prevent USAC from successfully verifying the reference. Incomplete entries or vague project details will result in the reference being excluded from evaluation, directly impacting the Offeror's risk rating.*

D. Price (Volume 4)

This volume must include:

1. A cover page, as outlined above.
2. Completed pricing information in Attachment 1 – Bid Sheet.
3. A separately priced alternate for platform-native external data publication in lieu of Socrata, if proposed, in accordance with Section B.6.6.
4. A separately priced alternate for an alternative archival architecture, if proposed, in accordance with Section B.6.9.
5. Identification of all cost drivers, consumption metrics, and the factors that materially increase or decrease cost, and identification of which Section B.6 capabilities require licensing separate from the core offering.
6. The cost model applicable to retrieving, exporting, or transferring USAC Data out of the platform, including any data egress or extract charges, together with recommended practices for minimizing them, and confirmation that no such charge applies to the return of USAC Data on transition.
7. Clear identification of which cost components are mandatory and which are optional, so that USAC may evaluate the optional components independently.
8. The cost structure for the Development, Test/QA and Pre-Production environments, stated separately from Production.
9. All proposed prices must be fully loaded and must include wages, overhead, general and administrative expenses, taxes, and profit.

8. PROPOSAL EVALUATION

USAC will award a single contract resulting from this solicitation to the responsible Offeror whose offer conforming to the solicitation will be most advantageous to USAC considering POC results, technical and price factors. The following factors shall be used to evaluate proposals and select the awardee – Technical, Experience & Past Performance, and Price.

Universal Service Administrative Co.

8.1. TECHNICAL:

The technical sub-factors listed below in descending order of importance:

A. Technical Approach
B. Capabilities
C. Key Personnel

A. Technical Approach: USAC will assess the soundness, completeness and realism of the proposed approach across all CLINs; the depth, thoroughness, and business justification of the proposed AI framework and its articulated benefits to USAC; the fit of the proposed platform to the requirements of Section B.6 as evidenced by the compliance matrix; the quality and rigor of the proposed POC approach; the credibility of the migration, reconciliation and cutover approach against the ~~mandatory floor~~minimum viable product; the treatment of the business intelligence and governance options; the geospatial approach; and the security and privacy approach, including the handling of production data in the final validation round. USAC will additionally assess the usability of the proposed platform for non-technical business users, the realism of the proposed division of work between Contractor and USAC, and the sustainability of the proposed platform having regard to the availability of implementation and support resources beyond the Offeror.

B. Capabilities: USAC will assess the Offeror's organizational capability to perform, including depth of resources, management capability, demonstrated experience with the proposed platform, and the adequacy of the proposed staffing model to sustain parallel POC execution and, if selected, full implementation and operations. USAC will carefully evaluate the risks associated with proposed teaming and subcontracting structures. Proposals reliant on overly fragmented delivery frameworks (such as teams utilizing more than two subcontractors) will be heavily scrutinized for operational integration risk, communication overhead, and accountability.

C. Key Personnel: USAC will assess the qualifications and relevant experience of each named Key Personnel against the requirements of Section B.~~14.1~~11.4 based upon the mandatory formal resumes submitted in Attachment ~~43~~, and the availability and continuity of those individuals.

8.2. EXPERIENCE & PAST PERFORMANCE

Past performance information will be evaluated to assess the risk associated with the Offeror's performance of this effort, considering relevance, recency (no older than three (3) years from the date of this solicitation), and quality of performance on past or current contracts for the same or similar services. Vague or incomplete past performance descriptions that fail to cleanly establish technical relevance, lack verifiable dollar values or exact durations, or contain personal contact info will be assigned a higher risk rating. USAC will prioritize references that demonstrate strong, verified industry capabilities external to USAC. USAC will consider information obtained from

references, from questionnaires, and from any other source, including government databases and contracts listed in the proposal that are not identified as references.

8.3. PRICE

USAC will evaluate total evaluated price comprising CLIN 0001 across the base and option years, CLIN 0002, and CLIN 0003 and the overall NTE ceiling and labor rates. USAC will evaluate whether proposed prices are realistic (reasonably sufficient to perform the requirements) and reasonable. Proposals containing prices determined to be unrealistic or unreasonable will not be considered for award.

9. PROOF OF CONCEPT, FINAL PROPOSAL REVISION, BEST AND FINAL OFFER

USAC will review the proposed POC Test Plan submitted with offeror's proposal and will request a POC from selected offerors during proposal evaluation, prior to contract award. After reviewing the initial proposal, USAC will contact selected offerors to submit their final POC Test Plan. The selected offerors will be provided with sufficient time, access to USAC systems as appropriate, and documentation needed to execute their POC. USAC will establish the numeric pass thresholds for each test case that will be applied to all participating offerors. After completion of POCs, USAC will contact the selected offerors to submit their Final Proposal Revision ("FPR") and Best and Final Offer ("BAFO"). USAC will review the POC test results, FPRs and BAFOs to make a final award determination. During proposal evaluation, USAC reserves the right to require and hold additional Q&A sessions, product/solution demonstrations and discussions with select Offerors. See Section B.20 for the POC requirements.

10. DOWN-SELECT PROCESS

USAC may determine that the number of proposals received is too numerous to efficiently conduct a full evaluation of all evaluation factors prior to establishing a competitive range. In such case, USAC may conduct a down-select to eliminate Offerors from further consideration based on a comparative analysis of proposals, with primary focus on the proposal completeness and price proposal, but USAC may in its sole discretion consider other factors including quality of proposal, technical capabilities and past performance. Proposals with proposed prices significantly higher than the median, or with prices unrealistically low in terms of sufficiency to perform, may be excluded from the competition without evaluation under the other evaluation factors.

11. ORGANIZATIONAL CONFLICT OF INTEREST

Offerors are advised that USAC has engaged third parties to conduct assessments of the existing EDW and of USAC's data management maturity. ~~Firms that performed those assessments shall not use the same resources to compete under this solicitation.~~ Consistent with the neutrality requirements applicable to USAC procurements, Offerors must identify any actual or potential conflicts of interest, or circumstances giving rise to the appearance of a conflict, and propose specific and detailed measures to avoid, neutralize or mitigate them. If USAC determines that a proposed mitigation plan does not

adequately address an actual, potential or apparent conflict of interest, the Offeror will not be eligible for award. The platform relationship disclosure required by Section E.~~6.1~~7.A.5 is in addition to, and does not substitute for, this requirement.

12. RESPONSIBILITY DETERMINATION

USAC will only award contracts to responsible Offerors. USAC will make a responsibility determination based on any available information, including information submitted in an Offeror's proposal. In making a responsibility determination, USAC will consider whether:

1. Offeror has sufficient financial and operational scale (as verified by corporate volume metrics including annual revenue and employee headcounts) to successfully mitigate performance risk over a high-value, multi-year contract.
2. Offeror has sufficient resources to perform the Services described in the RFP
3. Offeror has a satisfactory record of performance, integrity, and business ethics
4. Offeror has the accounting systems and internal controls, quality assurance processes, and organizational structure and experience necessary to assure that contract work will be properly performed and accurately invoiced
5. Offeror is not excluded from government contracting, as listed on the excluded parties list in https://www.sam.gov; and
6. Offeror has an active registration in https://www.sam.gov.